Oracle® Secure Global Desktop

Gateway 管理者ガイド (バージョン 4.6 用)

Part No. 821-2166-10
2010 年 8 月 , Revision 01

Copyright © 2010 Oracle and/or its affiliates. All rights reserved.
このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション（人的傷害を発生させる可能性があるアプリケーションを含む）への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

Oracle と Java は Oracle Corporation およびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

AMD、Opteron、AMD ロゴ、AMD Opteron ロゴは、Advanced Micro Devices, Inc. の商標または登録商標です。Intel、Intel Xeon は、Intel Corporation の商標または登録商標です。すべての SPARC の商標はライセンスをもとに使用し、SPARC International, Inc. の商標または登録商標です。UNIX は X/Open Company, Ltd. からライセンスされている登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

Please
Recycle

Adobe PostScript

目次

はじめに　xi

1.　SGD Gateway のインストール　1

SGD Gateway について　1

システム要件　2

既知の問題　2

インストールの実行　2

▼ SGD Gateway のインストール方法　3

SGD Gateway のアップグレード　5

▼ SGD Gateway のアップグレード方法　5

2.　SGD Gateway の設定　7

SGD Gateway の配備　7

基本的な配備　7

負荷分散された配備　9

SGD Gateway の設定作業　12

クライアントデバイスから SGD Gateway への接続　12

▼ SGD Gateway のポートと接続を設定する方法　12

▼ クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法　13

SGD Gateway から SGD サーバーへの接続　14

▼ SGD サーバーの証明書をインストールする方法　14
▼ SGD Gateway の証明書を SGD アレイにインストールする方法　16
▼ SGD Client 接続を設定する方法　17
クライアントデバイスからロードバランサへの接続　17
ロードバランサから SGD Gateway への接続　17
SGD Gateway の制御　18
SGD Gateway の起動　18
SGD Gateway の停止　18
SGD Gateway の再起動　19
SGD Gateway の削除　19
▼ SGD Gateway の削除方法　19

A. SGD Gateway のアーキテクチャーの概要　21

SGD Gateway のアーキテクチャー　21
SGD Gateway のコンポーネント　25
ルーティングトークンについて　25
SGD Gateway で使用されるキーストア　26
ルーティングプロキシ設定ファイル　27
Apache Web サーバーの設定ファイル　28
逆プロキシと負荷分散の設定　28
SGD Gateway で使用される Apache モジュール　29

B. コマンド行リファレンス　31

`gateway` コマンド　31
形式　31
説明　32
使用例　33
`gateway start`　33
形式　33

説明 33
使用例 33
gateway stop 33
形式 34
説明 34
使用例 34
gateway restart 34
形式 34
説明 34
使用例 34
gateway config 35
形式 35
説明 35
使用例 35
gateway config create 35
形式 36
説明 36
使用例 36
gateway config list 37
形式 37
説明 37
使用例 38
gateway config edit 38
形式 38
説明 38
使用例 39
gateway config enable 39
形式 40

説明 40
使用例 40
gateway config disable 41
形式 41
説明 41
使用例 42
gateway server 42
形式 42
説明 42
使用例 42
gateway server add 42
形式 43
説明 43
使用例 44
gateway server remove 44
形式 44
説明 44
使用例 44
gateway server list 45
形式 45
説明 45
使用例 45
gateway status 45
形式 45
説明 45
使用例 46
gateway version 46
形式 46

説明 46
使用例 46
gateway sslcert 46
形式 47
説明 47
使用例 47
gateway sslcert export 47
形式 47
説明 47
使用例 48
gateway sslcert print 48
形式 48
説明 48
使用例 48
gateway sslkey 48
形式 49
説明 49
使用例 49
gateway sslkey import 49
形式 50
説明 50
使用例 51
gateway sslkey export 51
形式 51
説明 51
使用例 52
gateway cert export 52
形式 52

説明 52
使用例 52
gateway key import 53
形式 53
説明 53
使用例 54
gateway setup 54
形式 54
説明 54
使用例 55
gateway uninstall 55
形式 55
説明 55
使用例 55
tarantella gateway コマンド 55
形式 56
説明 56
使用例 56
tarantella gateway add 57
形式 57
説明 57
使用例 57
tarantella gateway list 58
形式 58
説明 58
使用例 58
tarantella gateway remove 58
形式 58

説明　58
使用例　59
--security-gateway 属性　59

C.　詳細設定　63

SGD Gateway の調整　63
AIP 接続の最大数の変更　64
AIP 接続数の計算　64
HTTP 接続の最大数の変更　65
JVM のメモリーサイズの変更　65
JVM のメモリーサイズの計算　65
HTTP リダイレクトの設定　66
SGD Gateway のバインディングポートの変更　66
SGD アレイに対する非暗号化接続の使用　67
外部 SSL アクセラレータの使用　68
▼ 外部 SSL アクセラレータのサポートを有効にする方法　68
SGD Gateway でのクライアント証明書の使用法　69
▼ クライアント証明書が使用されるように SGD Gateway を設定する方法　69
Balancer Manager アプリケーションの有効化　70
リフレクションサービス　71
リフレクションサービスの有効化　71
▼ リフレクションサービスに対する無認証アクセスを有効にする方法　72
▼ リフレクションサービスに対する認証アクセスを有効にする方法　73
リフレクションサービスの使用　74
RESTful Web サービスについて　75
リフレクションサービスの使用例　76

D.　SGD Gateway のトラブルシューティング　79

ログと診断　79

SGD Gateway のログについて　79
ログレベルの変更　80
ログファイルの場所　80
SGD Gateway のプロセス情報の表示　81
コマンド行からの設定の確認　81
SGD Gateway のエラーメッセージ　82

はじめに

『 *Oracle Secure Global Desktop 4.6 Gateway 管理者ガイド* 』には、Oracle Secure Global Desktop Gateway (SGD Gateway) のインストール、設定、および操作の手順が記載されています。このマニュアルはシステム管理者向けに記述されています。

内容の紹介

第 1 章では、SGD Gateway のインストール方法について説明します。

第 2 章では、ネットワークに応じて SGD Gateway を設定する方法について説明します。

付録 A では、SGD Gateway のアーキテクチャーについて説明します。

付録 B では、コマンド行から SGD Gateway を設定および制御する方法について説明します。

付録 C では、SGD Gateway のリフレクションサービスの設定方法と使用方法など、SGD Gateway の高度な設定について説明します。

付録 D では、SGD Gateway の問題の診断と解決に役立つ、トラブルシューティング関連の情報について説明します。

UNIX コマンドの使用法

このマニュアルには、システムのシャットダウン、システムのブート、デバイスの設定といった基本的な UNIX® のコマンドや手順に関する情報は記載されていない場合があります。このような情報については、次のマニュアルを参照してください。

- 使用しているシステムに付属しているソフトウェアマニュアル
- Solaris™ オペレーティングシステムのマニュアル。次の場所から入手できます。

  http://docs.sun.com

ただし、それぞれの SGD コマンドに関する情報はこのマニュアルに記載されています。

シェルプロンプト

シェル	プロンプト
C シェル	*machine-name*%
C シェルスーパーユーザー	*machine-name*#
Bourne シェルおよび Korn シェル	$
Bourne シェルおよび Korn シェルスーパーユーザー	#

表記上の規則

字体	意味	使用例
AaBbCc123	コマンド名、ファイル名、およびディレクトリ名を示します。または、画面上のコンピュータ出力を示します。	.login ファイルを編集します。 ls -a を使用してすべてのファイルを表示します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力とは区別して示します。	% **su** Password:
AaBbCc123	書名、新規語や新規用語、強調する語句を示します。コマンド行の変数を示します。実際に使用する特定の名前または値で置き換えます。	『*ユーザーガイド*』の第 6 章を参照してください。 これらは*クラス*オプションと呼ばれます。 ファイルを削除するには、**rm** *filename* と入力します。

注 - ブラウザの設定によって、文字の表示が異なります。文字が正しく表示されない場合は、使用しているブラウザの文字エンコーディングを Unicode UTF-8 に変更してください。

関連マニュアル

次の表は、この製品に関するマニュアルの一覧を示しています。オンラインマニュアルは、次のサイトで参照できます。

http://docs.sun.com/app/docs/coll/1706.5

アプリケーション	タイトル	Part Number	形式	ロケーション
リリースノート	*Oracle Secure Global Desktop 4.6 Platform Support and Release Notes*	821-1928	HTML PDF	オンライン DVD メディアおよびオンライン
インストール	*Oracle Secure Global Desktop 4.6 インストールガイド*	821-2162	HTML PDF	オンライン DVD メディアおよびオンライン
管理	*Oracle Secure Global Desktop 4.6 管理者ガイド*	821-2167	HTML PDF	オンライン
ユーザー	*Oracle Secure Global Desktop 4.6 ユーザーガイド*	821-2157	HTML PDF	オンライン

マニュアルのフィードバック

このマニュアルに関するコメントは、http://docs.sun.com で Feedback[+] リンクをクリックして送付してください。フィードバックには、次のように、マニュアルのタイトルと Part Number を含めるようにしてください。

Oracle Secure Global Desktop 4.6 Gateway 管理者ガイド 、Part Number *821-2166*

第1章

SGD Gateway のインストール

この章では、Oracle Secure Global Desktop Gateway (SGD Gateway) の簡単な紹介に続き、SGD Gateway ソフトウェアのインストール方法について説明します。この章では、SGD Gateway のシステム要件の詳細についても説明します。

この章の内容は、次のとおりです。

- 1 ページの「 SGD Gateway について 」
- 2 ページの「 システム要件 」
- 2 ページの「 インストールの実行 」
- 5 ページの「 SGD Gateway のアップグレード 」

SGD Gateway について

SGD Gateway は、非武装ゾーン (DMZ) で SGD アレイの前に配備されるように設計されたプロキシサーバーです。これにより、組織の内部ネットワーク上に SGD アレイを配置できるようになります。また、アレイ内の SGD サーバーに接続する前に、すべての接続を DMZ で認証できます。

ファイアウォール越え (ファイアウォール転送とも呼ばれる) を使用して SGD サーバーを実行する代わりに、SGD Gateway を使用できます。

SGD Gateway はハイパーテキスト転送プロトコル (HTTP) 接続の負荷分散を管理するので、SGD に含まれている JavaServer Pages™ (JSP™) テクノロジの負荷分散ページを使用する必要はありません。

システム要件

SGD Gateway ホストでサポートされるインストールプラットフォームは、http://docs.sun.com/app/docs/doc/821-1928 で参照可能な『 *Oracle Secure Global Desktop 4.6 Platform Support and Release Notes* 』に一覧表示されています。

SGD Gateway とともに使用される SGD サーバーには、次の要件が適用されます。

- **セキュアモード。**デフォルトでは、SGD Gateway では SGD サーバーへのセキュア接続が使用されます。SGD サーバーでセキュア接続を有効にする必要があります。ファイアウォールの転送が無効になっている必要があります。

  SGD サーバーをセキュリティー保護する方法については、『 *Oracle Secure Global Desktop 4.6 管理者ガイド* 』の第 1 章の「 Secure Connections to SGD Servers 」を参照してください。
- **統合モード。**SGD Client は、統合モードで SGD サーバーにアクセスするように設定してはいけません。
- **SGD のバージョン。**SGD サーバーでは SGD version 4.5 以降が実行されている必要があります。SGD version 4.6 で Gateway version 4.6 を使用することをお勧めします。
- **クロックの同期。**SGD サーバーと SGD Gateway のシステムクロックが同期していることが重要です。時間情報プロトコル (NTP) ソフトウェアまたは `rdate` コマンドを使用して、クロックが同期していることを確認してください。

SGD サーバーのシステム要件については、『 *Oracle Secure Global Desktop 4.6 Platform Support and Release Notes* 』を参照してください。

既知の問題

SGD Gateway のこのリリースで認識されている問題の詳細については、『 *Oracle Secure Global Desktop 4.6 Platform Support and Release Notes* 』を参照してください。

インストールの実行

Solaris OS プラットフォームでは、`pkgadd` コマンドを使用して SGD Gateway をインストールします。

Linux プラットフォームでは、`rpm` コマンドを使用して SGD Gateway をインストールします。

デフォルトでは、SGD Gateway は /opt/SUNWsgdg ディレクトリにインストールされます。インストールディレクトリは、次のようにして変更できます。

- **Solaris OS プラットフォーム –** ソフトウェアのインストール時に、インストールプログラムによってインストールディレクトリの指定が求められます。
- **Linux プラットフォーム –** ソフトウェアのインストール時に rpm コマンドに --prefix オプションを使用することで、別のインストールディレクトリを選択できます。

▼ SGD Gateway のインスト ール方法

1. **ホスト上の一時ディレクトリに SGD Gateway パッケージを保存します。**

   インストールメディアからインストールする場合、パッケージは gateway ディレクトリにあります。

   または、インストールプログラムを SGD Web サーバー http://*server.example.com* からダウンロードします。ここで、*server.example.com* は SGD サーバーの名前です。SGD Web サーバーの開始画面が表示されたら、「 Oracle Secure Global Desktop Gateway のインストール」をクリックします。

   パッケージファイルは次のとおりです。

   - SUNWsgdg-*version*.sol-x86.pkg (x86 プラットフォーム版 Solaris OS)
   - SUNWsgdg-*version*.sol-sparc.pkg (SPARC テクノロジプラットフォーム版 Solaris OS)
   - SUNWsgdg-*version*.i386.rpm (Linux プラットフォーム)

   ここで、*version* は SGD Gateway のバージョン番号です。

2. **ホストにスーパーユーザー (root) としてログインします。**

3. **SGD Gateway をインストールします。**

   パッケージファイルが圧縮されている場合、インストール前にファイルを解凍する必要があります。

   x86 プラットフォーム版 Solaris OS にインストールする場合 :

```
# pkgadd -d /tempdir/SUNWsgdg-version.sol-x86.pkg
```

   SPARC テクノロジプラットフォーム版 Solaris OS にインストールする場合 :

```
# pkgadd -d /tempdir/SUNWsgdg-version.sol-sparc.pkg
```

注 - Solaris OS プラットフォームでは、「 `pwd: cannot determine current directory!` 」という エラーメッセージが表示されてインスト ールが失敗した場合は、*/tempdir* ディレクトリに移動して、インストールを再度実行してください。

Linux プラットフォームにインストールする場合 :

```
# rpm -Uvh /tempdir/SUNWsgdg-version.i386.rpm
```

4. SGD Gateway パッケージがパッケージデータベースに登録されていることを確認します。

Solaris OS プラットフォームの場合 :

```
# pkginfo -x SUNWsgdg
```

Linux プラットフォームの場合 :

```
# rpm -qa | grep -i SUNWsgdg
```

5. SGD Gateway のセットアッププログラムを実行します。

```
# /opt/SUNWsgdg/bin/gateway setup
```

SGD Gateway のセットアッププログラムは次の設定を提示します。ユーザーは、それを受け入れることも変更することもできます。

- **SGD Gateway のポート設定。**SGD Gateway で着信接続に使用されるインタフェースとポートです。デフォルトでは、SGD Gateway はすべてのインタフェースのポート 443 で待機します。
- **ネットワークエントリポイント。**クライアントデバイスが SGD Gateway に接続するために使用するインターネットプロトコル (IP) アドレスまたはドメインネームシステム (DNS) 名、およびポートです。これは、SGD Gateway のアドレスと常に同じであるとは限りません。ネットワークの構成によっては、ロードバランサなどの外部デバイスのアドレスになることがあります。

  たとえば、ユーザーが SGD Gateway `gateway1.example.com` に直接接続する場合は、ネットワークエントリポイントとして `gateway1.example.com:443` を入力します。

  ユーザーがロードバランサ `lb.example.com` を介して SGD Gateway に接続する場合は、ネットワークエントリポイントとして `lb.example.com:443` を入力します。
- **セキュア接続。**SGD Gateway とアレイ内の SGD サーバーとの接続をセキュリティー保護するかどうか。デフォルトでは、SGD Gateway はセキュア接続を使用します。セキュア続を使用するには、アレイ内の SGD サーバーがセキュアモードで稼働している必要があります。

注 - これらの設定は、あとで `gateway config create` コマンドを使用して変更できます。12 ページの「 SGD Gateway のポートと接続を設定する方法 」を参照してください。

ソフトウェアをインストールしたあと、SGD Gateway の追加の設定を実行する必要があります。実行する必要のある作業の詳細については、第 2 章を参照してください。

SGD Gateway のアップグレード

この節では、SGD Gateway のアップグレード方法について説明します。

SGD Gateway をアップグレードしても、キーストアやルーティングプロキシ設定ファイルなど、元の設定は保持されます。アップグレード後、SGD Gateway を再設定する必要はありません。

アップグレードログは、`/opt/SUNWsgdg/proxy/var/log/upgrade_`*oldversion*`_`*newversion*`.log` に作成されます。ここで、*oldversion* は SGD Gateway の古いバージョンで、*newversion* は SGD Gateway のアップグレードされたバージョンです。

アップグレード時には、SGD Gateway のインストールプログラムによって、検出されてアップグレードログに一覧表示された、カスタマイズ済みの Apache Web サーバーファイルがバックアップされます。これらのファイルは手動でアップグレードする必要があります。`diff` などのユーティリティーを使用して、ファイルを比較したり、加えられた変更を示したりすることができます。

▼ SGD Gateway のアップグレード方法

1. **SSGD Gateway を介して実行されているユーザーセッションやアプリケーションセッションがないことを確認します。**
2. **新しいバージョンの SGD Gateway をインストールします。**

   3 ページの「 SGD Gateway のインストール方法 」を参照してください。

第2章

SGD Gateway の設定

この章では、一般的な配備シナリオに対して Oracle Secure Global Desktop Gateway (SGD Gateway) を設定する方法について説明します。SGD Gateway の起動と停止の方法、および SGD Gateway ソフトウェアの削除方法についても説明します。

この章の内容は、次のとおりです。

- 7 ページの「 SGD Gateway の配備 」
- 12 ページの「 SGD Gateway の設定作業 」
- 18 ページの「 SGD Gateway の制御 」
- 19 ページの「 SGD Gateway の削除 」

SGD Gateway の配備

この節では、次に示す SGD Gateway の配備シナリオについて説明します。

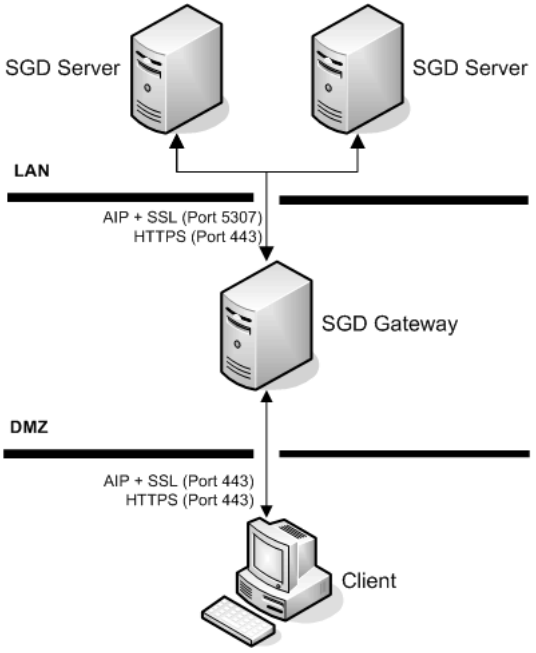
- 7 ページの「 基本的な配備 」
- 9 ページの「 負荷分散された配備 」

基本的な配備

ここでは、SGD Gateway の基本的な配備の設定作業について説明します。

基本的な配備では、単一の SGD Gateway を図 2-1 のように使用します。

図 2-1 単一の SGD Gateway を使用した基本的な配備



基本的な配備を設定するには、表 2-1 に示す接続の設定作業を行います。

表 2-1 SGD Gateway の基本的な配備で使用する接続

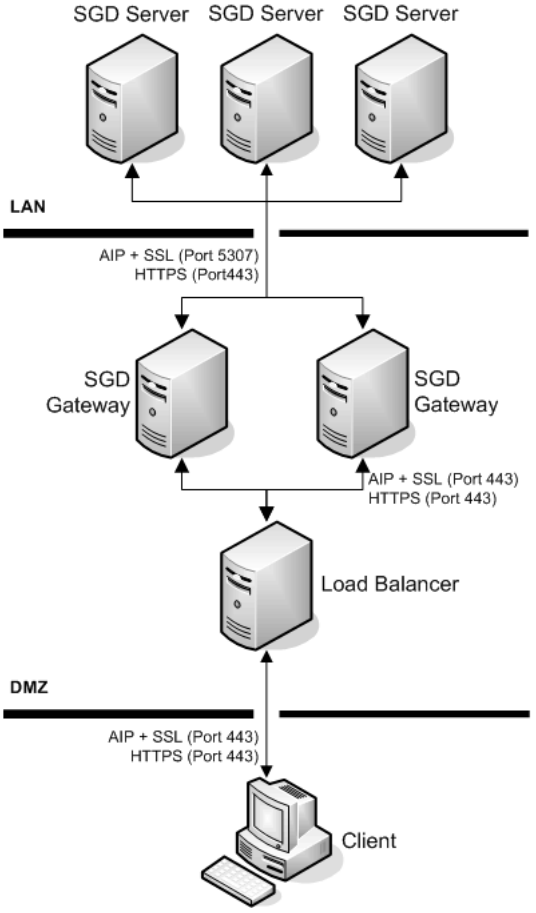
接続	設定手順
クライアントデバイスから SGD Gateway	1. SGD Gateway で使用するポートと接続を設定します。 これらの設定は、SGD Gateway のインストール時に行いました。 SGD Gateway の設定を変更する場合は、12 ページの「 SGD Gateway のポートと接続を設定する方法 」を参照してください。 2. SGD Gateway に、クライアント接続用の Secure Sockets Layer (SSL) 証明書をインストールします。 13 ページの「 クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法 」を参照してください。
SGD Gateway から SGD サーバー	1. アレイに対して SGD セキュリティーサービスを有効にします。 SGD サーバーはセキュアモードで稼働している必要があります。ファイアウォールの転送が無効になっている必要があります。 これを行う方法については、『 *Oracle Secure Global Desktop 4.6 管理者ガイド* 』の第 1 章の「 Secure Connections to SGD Servers 」を参照してください。 2. SGD Gateway に、SGD サーバーのセキュリティー証明書をインストールします。 `gateway server` コマンドを使用して、アレイ内の SGD サーバーの CA 証明書と SSL 証明書を SGD Gateway キーストアにインポートします。 14 ページの「 SGD サーバーの証明書をインストールする方法 」を参照してください。 3. SGD Gateway を使用するようにアレイ内の SGD サーバーを設定します。 SGD Gateway の証明書を SGD アレイにインストールし、`tarantella gateway add` コマンドを使用して SGD Gateway を SGD アレイに登録します。 16 ページの「 SGD Gateway の証明書を SGD アレイにインストールする方法 」を参照してください。 4. どの SGD Client 接続で SGD Gateway を使用できるかを設定します。 17 ページの「 SGD Client 接続を設定する方法 」を参照してください。

負荷分散された配備

ここでは、SGD Gateway の負荷分散された配備の設定作業について説明します。

負荷分散された配備では、複数の SGD Gateway とネットワークエントリポイントとなるロードバランサを図 2-2 のように使用します。

図 2-2 複数の SGD Gateway とロードバランサを使用したネットワーク配備



負荷分散された配備を設定するには、表 2-1 に示す接続の設定作業を行います。

表 2-2 SGD Gateway の負荷分散された配備で使用する接続

接続	設定作業
クライアントデバイスからロードバランサ	1. クライアントデバイスからの着信接続を有効にします。 通常、これには Transmission Control Protocol (TCP) ポート 443 を使用します。 この方法の詳細については、ロードバランサのマニュアルを参照してください。 2. (省略可能) ロードバランサに、SGD Gateway でクライアント接続に使用される SSL 証明書をインストールします。 この方法の詳細については、ロードバランサのマニュアルを参照してください。
ロードバランサから SGD Gateway	1. 接続を SGD Gateway に転送するようにロードバランサを設定します。 この方法の詳細については、ロードバランサのマニュアルを参照してください。 2. SGD Gateway で使用するポートと接続を設定します。 ネットワークエントリポイントをロードバランサのアドレスに設定します。 これらの設定は、SGD Gateway のインストール時に行いました。 SGD Gateway の設定を変更する場合は、12 ページの「 SGD Gateway のポートと接続を設定する方法 」を参照してください。 3. 各 SGD Gateway に、クライアント接続用の SSL 証明書をインストールします。 13 ページの「 クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法 」を参照してください。
SGD Gateway から SGD サーバー	1. SGD アレイに対して SGD セキュリティーサービスを有効にします。 SGD サーバーはセキュアモードで稼働している必要があります。ファイアウォールの転送が無効になっている必要があります。 これを行う方法については、『 *Oracle Secure Global Desktop 4.6 管理者ガイド* 』の第 1 章の「 Secure Connections to SGD Servers 」を参照してください。 2. SGD Gateway に、SGD サーバーのセキュリティー証明書をインストールします。 `gateway server` コマンドを使用して、アレイ内の SGD サーバーの CA 証明書と SSL 証明書を SGD Gateway キーストアにインポートします。 14 ページの「 SGD サーバーの証明書をインストールする方法 」を参照してください。 3. SGD Gateway を使用するようにアレイ内の SGD サーバーを設定します。 SGD Gateway の証明書を SGD アレイにインストールし、`tarantella gateway add` コマンドを使用して SGD Gateway を SGD アレイに登録します。 16 ページの「 SGD Gateway の証明書を SGD アレイにインストールする方法 」を参照してください。 4. どの SGD Client 接続で SGD Gateway を使用できるかを設定します。 17 ページの「 SGD Client 接続を設定する方法 」を参照してください。

SGD Gateway の設定作業

この節では、SGD Gateway で使用する接続を設定する手順について説明します。

説明する設定作業は次のとおりです。

- 12 ページの「 クライアントデバイスから SGD Gateway への接続 」
- 14 ページの「 SGD Gateway から SGD サーバーへの接続 」
- 17 ページの「 クライアントデバイスからロードバランサへの接続 」
- 17 ページの「 ロードバランサから SGD Gateway への接続 」

クライアント デバイスから SGD Gateway への接続

クライアントデバイスと SGD Gateway の間の接続を設定するには、次の設定作業を行います。

1. (省略可能) SGD Gateway で使用するポートと接続を設定します。

   これらの設定は、SGD Gateway のインストール時に行います。

   これらの設定を変更する場合は、12 ページの「 SGD Gateway のポートと接続を設定する方法 」を参照してください。

2. (省略可能) SGD Gateway に、クライアント接続用の SSL 証明書をインストールします。

   13 ページの「 クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法 」を参照してください。

▼ SGD Gateway のポートと接続を設定する方法

この手順を使用する必要があるのは、SGD Gateway のインストール時に行なった設定を変更する場合のみです。

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。

2. `gateway config create` コマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway config create
```

画面上の質問に回答して次の項目を設定します。

- **SGD Gateway のポート設定。**SGD Gateway で着信接続に使用されるインタフェースとポートです。

- **ネットワークエントリポイント。**クライアントデバイスが SGD Gateway に接続するために使用するインターネットプロトコル (IP) アドレスまたはドメインネームシステム (DNS) 名、およびポートです。これは、SGD Gateway のアドレスと常に同じであるとは限りません。ネットワークの構成によっては、ロードバランサなどの外部デバイスのアドレスになることがあります。
- **セキュア接続。**SGD Gateway とアレイ内の SGD サーバーとの接続をセキュリティー保護するかどうか。セキュア接続を使用するには、アレイ内の SGD サーバーがセキュアモードで稼働している必要があります。

3. 接続とポートの設定を保存します。

入力した設定を使用して SGD Gateway が設定されます。

▼ クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法

SGD Gateway でクライアント接続に使用される SSL 証明書は、SGD Gateway SSL 証明書と呼ばれます。SSL 証明書はクライアントキーストア `/opt/SUNWsgdg/proxy/etc/keystore.client` に保存されます。

デフォルトでは、SGD Gateway は*自己 署 名付き* SGD Gateway SSL 証明書をクライアント接続に使用しますが、この自己 署 名付き SSL 証明書を認証局 (CA) によって 署 名された証明書で置き換えることができます。

次の手順では、 CA によって 署 名された SSL 証明書があることを前提としています。

インストールする非公開鍵は Privacy Enhanced Mail (PEM) 形式で作成されている必要があります。

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。

2. SSL 証明書とそれに対応する非公開鍵を SGD Gateway ホストにコピーします。

3. SSL 証明書と非公開鍵をクライアントキーストアにインポートします。

`gateway sslkey import` コマンドを次のように使用します。

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile temp.key \
--keyalg RSA \
--certfile example.com.pem
```

ここでは、証明書ファイル *example.com.pem* と、それに対応する RSA で符号化された非公開鍵 *temp.key* がクライアントキーストアにインポートされます。

クライアントキーストア内の既存の自己 署 名付き SSL 証明書は上書きされます。

4. (省略可能) SGD Gateway を再起動します。

注意 - この手順は、SGD Gateway の初期設定を実行しない場合にのみ使用してください。初期設定のこの段階で SGD Gateway を再起動すると、SGD Gateway の初期設定が完了していないため、エラーメッセージが表示されます。

すでに設定済みで稼働している SGD Gateway の SSL 証明書を置き換える場合は、SGD Gateway を再起動します。

注 - SGD Gateway を再起動すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。

SGD Gateway ホストで、次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway restart
```

SGD Gateway から SGD サーバーへの接続

SGD Gateway とアレイ内の SGD サーバーとの接続では、相互承認のために証明書が使用されます。これらの接続を設定するには、次の設定作業を行います。

1. SGD サーバーの証明書を SGD Gateway にインストールします。

   14 ページの「 SGD サーバーの証明書をインストールする方法 」を参照してください。

2. SGD Gateway の証明書を SGD アレイにインストールします。

   16 ページの「 SGD Gateway の証明書を SGD アレイにインストールする方法 」を参照してください。

3. SGD Gateway に対する SGD Client 接続を設定します。

   17 ページの「 SGD Client 接続を設定する方法 」を参照してください。

▼ SGD サーバーの証明書をインストールする方法

この手順を使用するには、アレイ内の SGD サーバーがセキュアモードで稼働している必要があります。

SGD サーバーに対してセキュリティーサービスを有効にする方法については、『 *Oracle Secure Global Desktop 4.6 管理者ガイド* 』の第 1 章の「 Secure Connections to SGD Servers 」を参照してください。

アレイ内の各 SGD サーバーで、次の手順を繰り返します。

1. SGD ホストにスーパーユーザー (root) としてログインします。

2. **SGD サーバーから SGD Gateway キーストアディレクトリに CA 証明書をコピーします。**

   SGD サーバーの CA 証明書は、SGD ホストの `/opt/tarantella/var/info/certs/PeerCAcert.pem` にあります。

注 - この CA 証明書は、SGD サーバーがアレイ内のセキュア通信に使用するものと同じです。

   SGD Gateway キーストアディレクトリは `/opt/SUNWsgdg/proxy/etc` です。

   CA 証明書をコピーするときは、ファイルの内容や証明書ファイルがあった SGD サーバーを特定できるように、証明書ファイルの名前を変更することをお勧めします。

3. **SGD サーバーから SGD Gateway キーストアディレクトリに SSL 証明書をコピーします。**

   セキュアモードで稼働している SGD サーバーの SSL 証明書は、SGD ホストの `/opt/tarantella/var/tsp/cert.pem` にあります。

   SGD Gateway キーストアディレクトリは `/opt/SUNWsgdg/proxy/etc` です。

   SSL 証明書をコピーするときは、ファイルの内容や証明書ファイルがあった SGD サーバーを特定できるように、証明書ファイルの名前を変更することをお勧めします。

4. **SGD Gateway ホストにスーパーユーザー (root) としてログインします。**

5. **SGD Gateway キーストアに証明書をインポートします。**

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd-server1 \
--certfile /opt/SUNWsgdg/proxy/etc/PeerCAcert.pem --url https://sgd1.example.com \
--ssl-certfile /opt/SUNWsgdg/proxy/etc/cert.pem
```

   `--server` オプションは、証明書をキーストアに保存するときに使用する別名を定義します。この例では、CA 証明書は *sgd-server1* という別名で保存され、SSL 証明書は *sgd-server1-ssl* という別名で保存されます。

   https://sgd1.example.com は SGD Web サーバーの URL (Uniform Resource Locator) です。

6. **SGD Gateway を再起動します。**

注 - SGD Gateway を再起動すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。

   SGD Gateway ホストで、次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway restart
```

▼ SGD Gateway の証明書を SGD アレイにインストールする方法

各 SGD Gateway で、次の手順を繰り返します。

1. **SGD Gateway の証明書をエクスポートします。**

   a. **SGD Gateway ホストにスーパーユーザー (root) としてログインします。**

   b. **SGD Gateway キーストアから SGD Gateway の証明書をエクスポートします。**

      `gateway cert export` コマンドを次のように使用します。

```
# /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
```

      証明書がファイル *gateway1.pem* にエクスポートされます。

   c. **アレイのプライマリ SGD サーバーの `/opt/tarantella/var/tsp` ディレクトリに証明書をコピーします。**

      証明書をエクスポートするときは、証明書ファイルがあった SGD Gateway を特定できるように、証明書ファイルの名前を変更することをお勧めします。

   d. **Gateway の証明書でファイルへのアクセス権を変更します。**

```
# chmod 644 /opt/tarantella/var/tsp/gateway1.pem
```

2. **SGD Gateway を SGD アレイに登録します。**

   a. **プライマリ SGD サーバーにスーパーユーザー (root) としてログインします。**

   b. **SGD Gateway の証明書をインポートします。**

```
# tarantella gateway add --name sgd-gateway1 \
--certfile /opt/tarantella/var/tsp/gateway1.pem
```

      ここで、*sgd-gateway1* は SGD が SGD Gateway の識別に使用する名前、*gateway1.pem* は SGD Gateway の証明書ファイル名です。

      複数の SGD Gateway を同時に登録するには、`tarantella gateway add` コマンドの `--file` オプションを使用します。詳細については、55 ページの「 `tarantella gateway` コマンド 」を参照してください。

      `tarantella gateway add` を使用して行なった設定変更は、アレイ内のほかの SGD サーバーに複製されます。

▼ SGD Client 接続を設定する方法

- **SGD Gateway を使用する SGD Client 接続を設定します。**

  プライマリ SGD サーバーで `--security-gateway` グローバル属性を設定して、どの SGD Client が SGD Gateway を使用できるかをクライアントの IP アドレスまたは DNS 名に基づいて定義します。

  単一の SGD Gateway `gateway1.example.com` の TCP ポート 443 を介してすべての SGD Client 接続をルーティングするように指定するには、次のコマンドを使用します。

```
$ tarantella config edit --security-gateway \
"*:sgdg:gateway1.example.com:443"
```

  外部ロードバランサ `lb.example.com` の TCP ポート 443 を介してすべての SGD Client 接続をルーティングするように指定するには、次のコマンドを使用します。

```
$ tarantella config edit --security-gateway \
"*:sgdg:lb.example.com:443"
```

注 - `--security-gateway` 属性に加えた変更は、アレイ内のすべての SGD サーバーに適用されます。変更が反映されるのは、新規ユーザーセッションだけです。

  `--security-gateway` 属性を使用して複数の SGD Client 接続フィルタを定義する方法については、59 ページの「 `--security-gateway` 属性 」を参照してください。

クライアント デバイスからロード バランサへの接続

クライアントデバイスと外部ロードバランサの間の接続を設定するには、次の設定作業を行います。

1. クライアント デバイスからの接続を受け入れるよう にロード バランサを設定します。

   この方法の詳細については、ロードバランサのマニュアルを参照してください。

2. (省略可能) SGD Gateway の SSL 証明書をロード バランサにインスト ールします。

   この方法の詳細については、ロードバランサのマニュアルを参照してください。

ロードバランサから SGD Gateway への接続

外部ロードバランサと SGD Gateway の間の接続を設定するには、次の設定作業を行います。

1. SGD Gateway で使用するポートと接続を設定します。

   12 ページの「 SGD Gateway のポートと接続を設定する方法 」を参照してください。

2. (省略可能) SGD Gateway に、着信クライアント接続用の SSL 証明書をインストールします。

   13 ページの「 クライアント接続用の SSL 証明書をクライアントキーストアにインストールする方法 」を参照してください。

SGD Gateway の制御

この節では、SGD Gateway の制御方法について説明します。説明する作業は次のとおりです。

- SGD Gateway の起動
- SGD Gateway の停止
- SGD Gateway の再起動

SGD Gateway の起動

SGD Gateway を起動するには、次のコマンドを使用します。

```
# /opt/SUNWsgdg/bin/gateway start
```

SGD Gateway の停止

注意 - SGD Gateway を停止すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。つまり、SGD Gateway が予期せず停止された場合は、アプリケーションデータが失われる可能性があります。

SGD Gateway を停止するには、次のコマンドを使用します。

```
# /opt/SUNWsgdg/bin/gateway stop
```

gateway stop コマンドを使用すると、SGD Gateway を停止するかどうかの確認を求める警告メッセージが表示されます。このメッセージを表示しないようにするには、gateway stop コマンドの --force オプションを使用してください。

注 - SGD Gateway が停止している場合、ネットワークの外部のユーザーが SGD Gateway を使用して SGD に接続することはできません。--security-gateway 属性を使用して、クライアントデバイスが SGD Gateway を経由せずに直接 SGD にアクセスできるようにした場合、このようなクライアントデバイスは引き続き SGD にアクセスできます。59 ページの「 --security-gateway 属性 」を参照してください。

SGD Gateway の再起動

注意 - SGD Gateway を再起動すると、SGD Gateway を介して実行されているユーザーセッションとアプリケーションセッションはすべて切断されます。つまり、SGD Gateway が予期せず再起動された場合は、アプリケーションデータが失われる可能性があります。

SGD Gateway を再起動するには、次のコマンドを使用します。

```
# /opt/SUNWsgdg/bin/gateway restart
```

gateway restart コマンドを使用すると、SGD Gateway を停止するかどうかの確認を求める警告メッセージが表示されます。このメッセージを表示しないようにするには、gateway restart コマンドの --force オプションを使用してください。

SGD Gateway の削除

SGD Gateway を削除するには、SGD Gateway ホストにインストールされているソフトウェアを削除します。

▼ SGD Gateway の削除方法

1. **SGD Gateway ホストにスーパーユーザー (root) としてログインします。**
2. **SGD アレイの SGD Client のルーティング設定を変更します。**

a. プライマリ SGD サーバーにスーパーユーザー (root) としてログインします。

b. SGD アレイの `--security-gateway` 属性を編集します。

単一の SGD Gateway を使用した基本的な配備の場合は、次のコマンドを実行します。

```
# tarantella config edit --security-gateway ""
```

注 - 複数の SGD Gateway と外部ロードバランサを使用した負荷分散された配備の場合、`--security gateway` 属性を編集する必要はありません。

---

3. SGD Gateway をアンインストールします。

次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway uninstall
```

SGD Gateway を停止するかどうかの確認を求める警告メッセージが表示されます。

注意 - SGD Gateway の削除方法としてサポートされているのは、`gateway uninstall` コマンドだけです。`pkgrm` コマンドや `rpm` コマンドを使用して SGD Gateway を直接削除しないでください。

---

4. (省略可能) SGD アレイに登録されている SGD Gateway のリストから、この SGD Gateway を削除します。

a. SGD アレイに登録されている SGD Gateway を表示します。

```
# tarantella gateway list
Installed gateway: gateway1.example.com
Issuer: CN=gateway1.example.com, OU=Marketing, O=Example, L=Boston, ST=
Massachusetts, C=US
Serial Number: 1208509056
Subject: CN=gateway2.example.com, OU=Marketing, O=Example, L=Boston, ST=
Massachusetts, C=US
Valid from Fri Sep 26 09:57:36 GMT 2008 to Thu Dec 25 09:57:36 GMT 2008
```

b. SGD アレイに登録されている SGD Gateway のリストから、この SGD Gateway を削除します。

```
# tarantella gateway remove --name gateway1.example.com
```

付録 A

SGD Gateway のアーキテクチャーの概要

この章では、Oracle Secure Global Desktop Gateway (SGD Gateway) のアーキテクチャーと主なコンポーネントについて説明します。

この章の内容は、次のとおりです。

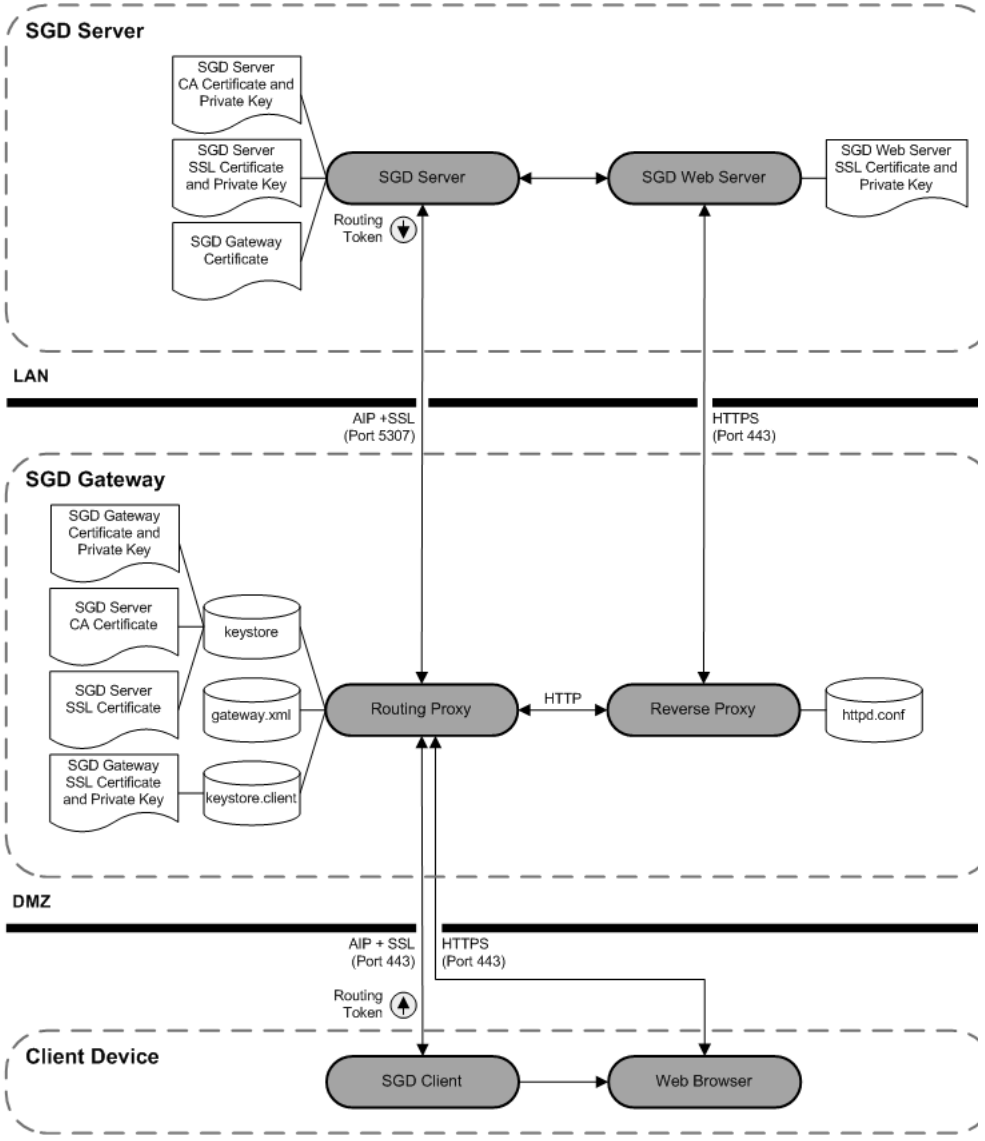
- 21 ページの「 SGD Gateway のアーキテクチャー 」
- 25 ページの「 SGD Gateway のコンポーネント 」

SGD Gateway のアーキテクチャー

この節では、SGD Gateway のアーキテクチャーを示し、SGD Gateway を介して SGD を実行するときに確立される接続について説明します。

図 A-1 に、SGD Gateway のアーキテクチャーを示します。

図 A-1 SGD Gateway のアーキテクチャー



SGD Gateway のアーキテクチャーを示すネットワーク図

次の手順では、SGD Gateway を介して SGD にアクセスするときに確立される接続について説明します。この手順では、ブラウザを使用した SGD への初期接続、SGD へのログオン、さらにアプリケーションの起動までが示されています。

1. クライアントデバイスのブラウザが SGD Gateway に対して Transmission Control Protocol (TCP) ポート 443 で HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) 接続を行います。

- 基本的な配備の場合、ユーザーは SGD Gateway の URL (Uniform Resource Locator) にアクセスすることによって SGD にアクセスできます。
- TCP ポート 443 は SGD Gateway のデフォルトポートです。SGD Gateway が使用するポートは、ルーティングプロキシ設定ファイル `gateway.xml` で定義されます。このファイルは、SGD Gateway のインストール時に自動的に作成され、`gateway config` コマンドを使用して SGD Gateway の設定を変更したときに更新されます。
- SGD Gateway は SSL 証明書を提示します。この証明書は、SGD Gateway の `keystore.client` キーストアにある唯一のエントリです。
- SGD Gateway が使用するキーストアの場所とパスワードは、ルーティングプロキシ設定ファイル `gateway.xml` で定義されます。

2. ルーティングプロキシは HTTPS 接続を認識し、データストリームを復号化し、HTTP データを Apache 逆プロキシに転送します。
   - ハイパーテキスト転送プロトコル (HTTP) データは、TCP ポート 8080 より上の最初の空きポートに内部で送信されます。
   - Apache 逆プロキシの設定は `httpd.conf` ファイルで定義されます。このファイルとそれに関連する逆プロキシ設定ファイルは、SGD Gateway のインストール時に自動的に作成されます。これらのファイルは、`gateway config` コマンドを使用して SGD Gateway の設定を変更したときに更新されます。
3. 逆プロキシは HTTP 負荷分散を使用して、アレイ内の SGD Web サーバーを選択します。
   - 逆プロキシと SGD Web サーバーの間の接続は、TCP ポート 443 で HTTPS を使用してセキュリティー保護されます。
   - Apache 逆プロキシはブラウザに負荷分散 Cookie を設定します。これ以降、ブラウザによるすべての HTTP 要求で同じ SGD Web サーバーが使用されます。
4. SGD Web サーバーはクライアントデバイスのブラウザに HTML を配信します。
   - HTML は、SGD Gateway の TCP ポート 443 に確立された接続上で、HTTPS データとして送信されます。
   - SGD Gateway は HTTPS データをブラウザに転送します。
5. ユーザーが SGD にログインします。
   - SGD サーバーはユーザーを認証し、ユーザーセッションを管理する SGD サーバーを選択し、新しいユーザーセッションを開始します。
   - クライアントデバイスに SGD Client がダウンロードおよびインストールされ、起動されます。
   - ブラウザに送信された HTML にルーティングトークンが含まれています。ルーティングトークンには、ユーザーセッションを管理するように選択された SGD サーバーのアドレスが含まれています。この情報は、AIP (Adaptive Internet Protocol) データを正しい SGD サーバーにルーティングするために使用されます。

- ルーティングトークンは、SGD サーバーの非公開鍵を使用して署名されたあと、SGD サーバーにある SGD Gateway の証明書を使用して暗号化されます。
- ルーティングトークンは SGD Client に渡されます。
- クライアントデバイスへの接続では HTTPS が使用されます。

6. SGD Client は SGD Gateway に TCP ポート 443 で接続します。
   - SGD Client と SGD Gateway の間のデータ接続では、AIP over Secure Sockets Layer (SSL) が使用されます。
   - SGD Gateway の SSL 証明書が接続のために提示されます。
   - ルーティングプロキシは AIP over SSL 着信データを認識します。
   - SSL データストリームが復号化され、AIP データストリームからルーティングトークンが抽出されます。
   - ルーティングトークンは、SGD Gateway の非公開鍵を使用して復号化されたあと、SGD サーバーの CA 証明書を使用して確認されます。
   - SGD Gateway の非公開鍵と SGD サーバーの CA 証明書は、SGD Gateway キーストア `keystore` に保存されています。
   - ルーティングトークンが有効であることを確認するために、ルーティングトークンのタイムスタンプが検査されます。
   - SSL を使用して AIP データストリームが再度暗号化されます。
7. AIP over SSL データはルーティングプロキシを介して、ルーティングトークンで指定されている SGD サーバーに転送されます。
   - AIP over SSL データ接続では TCP ポート 5307 が使用されます。
   - AIP データストリームにはルーティングトークンは含まれていません。
8. ユーザーが SGD Webtop でアプリケーションを起動します。
   - アプリケーションの起動要求は HTTPS を使用して SGD Gateway に送信されます。
   - ルーティングプロキシは HTTPS データを認識して復号化し、HTTP トラフィックを Apache 逆プロキシに転送します。
   - 逆プロキシは負荷分散 Cookie を検出し、Cookie で指定されている SGD Web サーバーを使用します。
   - SGD アプリケーションセッションの負荷分散では、アプリケーションセッションを管理するために同じ SGD サーバーが選択されます。
   - SGD サーバー上で新しいルーティングトークンが作成されます。ルーティングトークンは、アプリケーションセッションを管理するように選択された SGD サーバーに AIP データをルーティングするために使用されます。
   - SGD サーバーはルーティングトークンを SGD Client に送信します。既存の AIP データストリームにはルーティングトークンが含まれています。
9. SGD Client は SGD Gateway に TCP ポート 443 で接続します。

- SGD Gateway の SSL 証明書が接続のために提示されます。
- ルーティングプロキシは AIP over SSL 着信データを認識します。
- ルーティングトークンの復号化、確認、および検証が行われます。
- AIP over SSL データはルーティングプロキシを介して、ルーティングトークンで指定されている SGD サーバーに転送されます。
- AIP データストリームにはルーティングトークンは含まれていません。

10. SGD サーバーはアプリケーションセッションを管理します。
    - アプリケーションは、ローカルエリアネットワーク (LAN) に配置されたアプリケーションサーバー上で実行されます。

SGD Gateway のコンポーネント

SGD Gateway は次のコンポーネントで構成されます。

- **ルーティングプロキシ**。AIP データ接続を SGD サーバーにルーティングする、Java™ テクノロジベースのアプリケーションです。

  ルーティングプロキシの主要コンポーネントは次のとおりです。

  - ルーティングトークン – 25 ページの「ルーティングトークンについて」を参照
  - キーストア – 26 ページの「SGD Gateway で使用されるキーストア」を参照
  - ルーティングプロキシ設定ファイル – 27 ページの「ルーティングプロキシ設定ファイル」を参照
- **逆プロキシ。**逆プロキシモードで動作するように設定された Apache Web サーバーです。逆プロキシは HTTP 接続の負荷分散も実行します。

  逆プロキシの主要コンポーネントは次のとおりです。

  - Apache Web サーバーの設定ファイル – 28 ページの「Apache Web サーバーの設定ファイル」を参照
  - 逆プロキシ用および HTTP 負荷分散用の Apache モジュール – 29 ページの「SGD Gateway で使用される Apache モジュール」を参照

ルーティングトークンについて

SGD Gateway は*ルーティングトークン*を使用して AIP 接続を管理します。ルーティングトークンは、経路の送信元および送信先の SGD サーバーを識別する、署名され暗号化されたメッセージです。ルーティングトークンにはタイムスタンプが含まれており、トークンの寿命を制限するために使用されます。

発信ルーティングトークンは次のようになります。

- SGD サーバーの非公開鍵を使用して SGD サーバー上で 署 名されます。
- SGD Gateway の証明書を使用して SGD サーバー上で暗号化されます。
- クライアントデバイスの SGD Client に送信されます。

着信ルーティングトークンは次のようになります。

- SGD Gateway の非公開鍵を使用して SGD Gateway 上で復号化されます。
- 送信元 SGD サーバーの CA 証明書を使用して SGD Gateway 上で確認されます。
- SGD Gateway 上で破棄されます。ルーティングトークンを提示している接続は、送信先 SGD サーバーにルーティングされます。

SGD Gateway で使用されるキーストア

SGD Gateway は非公開鍵と証明書を使用して、ルーティングトークンへのデジタル署 名 、ルーティングトークンの確認、アレイ内の SGD サーバーに対する接続のセキュリティー保護、SGD Gateway へのクライアント接続のセキュリティー保護、およびリフレクションサービスへのアクセスの承認を行います。

SGD Gateway で使用される証明書と非公開鍵は、`/opt/SUNWsgdg/proxy/etc` ディレクトリのキーストアに保存されています。

このディレクトリには次のキーストアがあります。

- **SGD Gateway キーストア** `keystore` には、SGD Gateway の証明書と非公開鍵、アレイ内の SGD サーバーの CA 証明書、および SGD サーバーの SSL 証明書があり 、アレイ内の SGD サーバーに対するセキュア接続に使用されます。

  SGD Gateway キーストアのエントリを追加 、削除 、および一覧表示するには 、`gateway` コマンドを使用します。
- **クライアントキーストア** `keystore.client` には、単一の SGD Gateway SSL 証明書と非公開鍵があり 、クライアントデバイスと SGD Gateway の間の接続をセキュリティー保護するために使用されます。デフォルトでは、このキーストアには自己 署 名付き証明書が入っています。この証明書を認証局 (CA) によって 署 名された証明書で置き換えることができます。
- **リフレクションサービスキーストア** `keystore.reflection` には、SGD Gateway でリフレクションサービスへのアクセスの承認に使用される証明書と非公開鍵が含まれています。デフォルトでは、このキーストアには自己 署 名付き証明書と非公開鍵が入っています。

キーストアは、SGD Gateway のインストール後に `gateway setup` コマンドを実行したときに自動的に作成されます。

注 - すべてのキーストアで同じパスワードが使用されます。このパスワードは /opt/SUNWsgdg/etc/password ファイルで定義されます。このパスワードは、キーストアの最初の作成時に自動的に作成されるランダムなパスワードです。パスワードファイルを読み取ることができるのはスーパーユーザー (root) だけです。

ルーティングプロキシ設定ファイル

ルーティングプロキシ設定ファイルは /opt/SUNWsgdg/etc/gateway.xml です。これは、データプロトコルの種類に応じて経路を設定する XML ファイルです。ルーティングおよび SSL プロトコルに必要なキーストアの場所とパスワードも、このファイルで設定されます。

ルーティングプロキシ設定ファイルは、SGD Gateway のインストール時に自動的に作成され、gateway config コマンドを使用して SGD Gateway の設定を変更したときに更新されます。

注意 - gateway.xml ファイルを手動で編集しないでください。このファイルの設定が間違っていると、SGD Gateway が動作しなくなることがあります。

デフォルトのルーティングプロキシ設定ファイルは /opt/SUNWsgdg/etc/password ファイル内のパスワードを使用して、SGD Gateway が使用するキーストアにアクセスします。このパスワードをディスクに保存したくない場合は、パスワードファイル内のエントリを書きとめます。パスワードファイルを削除し、gateway.xml ファイルからすべての <keystore> 要素の password エントリを削除します。次に SGD Gateway を起動するとき、キーストアパスワードの入力を求められます。

SGD Gateway が使用するキーストアのパスワードを変更するには、keytool コマンドの -storepasswd オプションを使用します。たとえば、keystore.client キーストアのパスワードを変更するには、次のコマンドを実行します。

```
# /opt/SUNWsgdg/java/default/bin/keytool -storepasswd \
-keystore /opt/SUNWsgdg/proxy/etc/keystore.client
```

注 - /opt/SUNWsgdg/etc ディレクトリには、ほかの .xml ファイルと .template ファイルもあります。これらのファイルは、gateway config コマンドで gateway.xml ファイルを更新するために内部的に使用されます。これらのファイルを手動で編集しないでください。

Apache Web サーバーの設定ファイル

SGD Gateway で使用するために設定された Apache Web サーバーの設定ファイルは、/opt/SUNWsgdg/httpd/apache-version/conf ディレクトリにあります。

このディレクトリにある設定ファイルは、Apache Web サーバーの逆プロキシ処理と負荷分散を設定するために使用されます。

逆プロキシと負荷分散の設定

逆プロキシ処理と負荷分散を設定するためのファイルは、extra/gateway サブディレクトリにあります。これらのファイルは、メインの httpd.conf ファイルで次の Include 指令によって有効にされます。

```
# SGD Reverse Proxy/Load Balance settings
Include conf/extra/gateway/httpd-gateway.conf
```

httpd-gateway.conf ファイルは、Apache Web サーバーの逆プロキシと負荷分散を設定します。負荷分散グループのメンバーは、httpd-gateway.conf ファイルで次のように Include 指令を使用して定義されます。

```
<Proxy Balancer://mysgdservers/>
Include conf/extra/gateway/servers/*.conf
</Proxy>
```

extra/gateway/servers ディレクトリには、負荷分散グループの各 SGD Web サーバーの設定ファイルがあります。設定ファイルには *server-name*.conf という名前が付けられます。ここで、*server-name* は gateway server add コマンドで使用されたサーバー名です。このコマンドの詳細については、42 ページの「 gateway server add 」を参照してください。

SGD Gateway では*スティッキーセッション* HTTP 負荷分散が使用されます。つまり、Apache 逆プロキシはクライアントのブラウザに Cookie を設定することによって、ブラウザが必ず負荷分散で選択された SDG Web サーバーに戻るようにします。ユーザーセッションの終了時に Cookie は期限切れになります。

スティッキーセッションの Cookie は、httpd-gateway.conf ファイルで次のように Header add Set-Cookie 指令によって有効にされます。

```
Header add Set-Cookie "BALANCEID=balanceworker.%{BALANCER_WORKER_ROUTE}e; path=
/" env=BALANCER_ROUTE_CHANGED
```

ここで、BALANCEID は Cookie の名前、BALANCER_WORKER_ROUTE と BALANCER_ROUTE_CHANGED は Apache mod_proxy_balancer モジュールによってエクスポートされた環境変数です。これらの環境変数については、Apache mod_proxy_balancer のドキュメントを参照してください。

SGD Gateway で使用される Apache モジュール

SGD Gateway に付属の Apache Web サーバーでは、逆プロキシと負荷分散のために標準の Apache モジュールが使用されます。モジュールは DSO (Dynamic Shared Object) モジュールとしてインストールされます。

これらのモジュールは、/opt/SUNWsgdg/httpd/apache-version/conf/httpd.conf にある Apache 設定ファイル httpd.conf で、LoadModule 指令によって有効にされます。

付録 B

コマンド行リファレンス

この章では、コマンド行から Oracle Secure Global Desktop Gateway (SGD Gateway) の設定を管理、制御、および変更する方法について説明します。

キーストアと証明書の設定、SGD Gateway で使用するポートの設定、アレイ内の SGD サーバーに対する負荷分散の設定といった作業のためのコマンドが提供されています。

この章の内容は、次のとおりです。

- 31 ページの「 gateway コマンド 」
- 55 ページの「 tarantella gateway コマンド 」
- 59 ページの「 --security-gateway 属性 」

gateway コマンド

gateway コマンドは、SGD Gateway の設定と制御に使用します。

注 - gateway コマンドのフルパスは /opt/SUNWsgdg/bin/gateway です。

形式

```
gateway start | stop | restart | config | server | status | setup | version |
sslcert | sslkey | cert | key | setup | uninstall
```

説明

使用可能な gateway コマンドを次の表に示します。

コマンド	説明	詳細情報
gateway start	SGD Gateway を起動します	33 ページの「 gateway start 」
gateway stop	SGD Gateway を停止します	33 ページの「 gateway stop 」
gateway restart	SGD Gateway を停止してから再起動します	34 ページの「 gateway restart 」
gateway config	SGD Gateway を設定し、Apache 逆プロキシ設定ファイルを更新します	35 ページの「 gateway config 」
gateway server	SGD サーバーのセキュリティー証明書をインストールし、SGD アレイの負荷分散を設定します	42 ページの「 gateway server 」
gateway status	SGD Gateway の現在のステータスを表示します	45 ページの「 gateway status 」
gateway version	SGD Gateway のバージョン番号を表示します	46 ページの「 gateway version 」
gateway sslcert	クライアントキーストア内の Secure Sockets Layer (SSL) 証明書をエクスポートし、出力します	46 ページの「 gateway sslcert 」
gateway sslkey	クライアントキーストア内の非公開鍵と証明書を管理します	48 ページの「 gateway sslkey 」
gateway cert export	SGD Gateway キーストアから SGD Gateway の証明書をエクスポートします	52 ページの「 gateway cert export 」
gateway key import	非公開鍵と証明書を SGD Gateway キーストアにインポートします	53 ページの「 gateway key import 」
gateway setup	SGD Gateway のセットアッププログラムを実行します	54 ページの「 gateway setup 」
gateway uninstall	SGD Gateway ソフトウェアをアンインストールします	55 ページの「 gateway uninstall 」

注 - どの gateway コマンドにも --help オプションがあります。このオプションを使用すると、コマンドのヘルプを表示できます。

使用例

次の例では、SGD Gateway を起動します。

```
# /opt/SUNWsgdg/bin/gateway start
```

次の例では、SGD サーバー server.example.com は SGD Gateway の使用を承認されません。

```
# /opt/SUNWsgdg/bin/gateway server remove --server server.example.com
```

gateway start

SGD Gateway を起動します。

形式

```
gateway start
```

説明

SGD Gateway を起動します。

使用例

次の例では、SGD Gateway を起動します。

```
# /opt/SUNWsgdg/bin/gateway start
SGD Gateway started successfully
```

gateway stop

SGD Gateway を停止します。

形式

```
gateway stop [--force]
```

説明

ユーザーに確認を求めてから SGD Gateway を停止します。

`--force` オプションは、確認を求めずに SGD Gateway を停止します。

使用例

次の例では、ユーザーに確認を求めてから SGD Gateway を停止します。

```
# /opt/SUNWsgdg/bin/gateway stop
```

gateway restart

SGD Gateway を停止してから再起動します。

形式

```
gateway restart [--force]
```

説明

SGD Gateway を停止してから再起動します。SGD Gateway を停止する前に、ユーザーに確認を求めます。

`--force` オプションは、確認を求めずに SGD Gateway を停止します。

使用例

次の例では、ユーザーに確認を求めてから SGD Gateway を停止し、再起動します。

```
# /opt/SUNWsgdg/bin/gateway restart
```

gateway config

SGD Gateway を設定します。gateway config コマンドは、SGD Gateway のセキュア接続、ポート、および逆プロキシサーバーを設定します。

形式

```
gateway config create | show
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
create	SGD Gateway の新しい設定を作成します	35 ページの「 gateway config create 」
list	SGD Gateway の現在の設定を一覧表示します	37 ページの「 gateway config list 」
edit	SGD Gateway の現在の設定を編集します	38 ページの「 gateway config edit 」
enable	SGD Gateway のサービスを有効にします	39 ページの「 gateway config enable 」
disable	SGD Gateway のサービスを無効にします	41 ページの「 gateway config disable 」

使用例

次の例では、SGD Gateway の現在の設定を一覧表示します。

```
# /opt/SUNWsgdg/bin/gateway config list
```

gateway config create

SGD Gateway の新しい設定を作成します。現在の設定は上書きされます。

形式

```
gateway config create { [ --interface interface:port ]
                        [ --entry-point ip-address:port ]
                        [ --out plaintext | ssl ]
                      } | --file file
```

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--interface`	SGD Gateway が着信プロキシ接続を待機するインタフェースとポート。デフォルトは、すべてのインタフェースの Transmission Control Protocol (TCP) ポート 443 です。
`--entry-point`	ネットワークのエントリポイント。これは、クライアントが SGD Gateway に接続するために使用するインターネットプロトコル (IP) アドレスとポートです。IP アドレスの代わりにドメインネームシステム (DNS) アドレスを指定することもできます。
`--out`	SGD Gateway からアレイ内の SGD サーバーへの発信トラフィックの形式。セキュア接続を使用している場合は、`ssl` を選択してください。
`--file`	設定を含んでいるファイルを指定します。

注 - オプションを指定せずに `gateway config create` コマンドを使用すると、一連のオンラインプロンプトが表示されるので、必要な設定を入力できます。

`gateway config create` に `--file` オプションを使用する場合、指定するファイルは `/opt/SUNWsgdg/etc/gatewayconfig.xml` ファイルと同じ形式でなければいけません。12 ページの「 SGD Gateway のポートと接続を設定する方法 」で説明されているように、このファイルは SGD Gateway の初期設定時に作成されます。

使用例

次の例では、192.168.0.1 で、ネットワークエントリポイントからの接続を TCP ポート 443 で待機するように SGD Gateway を設定します。セキュア接続は、SGD Gateway とアレイ内の SGD サーバーの間で使用されます。

```
# /opt/SUNWsgdg/bin/gateway config create --interface *:443 \
--entry-point 192.168.0.1:443 --out ssl
```

gateway config list

SGD Gateway の現在の設定を一覧表示します。

形式

```
gateway config list [ --binding ]
                    [ --routes-http-maxcon ]
                    [ --routes-aip-maxcon ]
                    [ --routes-reverseproxy-redirect ]
                    [ --services-reflection-binding ]
                    [ --services-reflection-auth-binding ]
```

説明

コマンド行オプションを使用すると、特定の設定を一覧表示できます。オプションを指定しないと、SGD Gateway の設定の詳細がすべて表示されます。

SGD Gateway の現在の設定は `/opt/SUNWsgdg/etc/gatewayconfig.xml` ファイルに保存されています。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--binding`	SGD Gateway が着信プロキシ接続を待機するインタフェースとポート
`--routes-http-maxcon`	ハイパーテキスト転送プロトコル (HTTP) 接続の最大数
`--routes-aip-maxcon`	Adaptive Internet Protocol (AIP) 接続の最大数
`--routes-reverseproxy-redirect`	HTTP リダイレクトポート
`--services-reflection-binding`	SGD Gateway リフレクションサービスに対する無認証アクセスに使用されるインタフェースとポート
`--services-reflection-auth-binding`	SGD Gateway リフレクションサービスに対する認証アクセスに使用されるインタフェースとポート

使用例

次の例では、 SGD Gateway のバインディング設定と AIP 接続の最大数を表示します。

```
# /opt/SUNWsgdg/bin/gateway config list --binding --routes-aip-maxcon
binding: *:443
routes-aip-maxcon: 2920
```

次の例では、SGD Gateway の現在の設定の詳細をすべて表示します。

```
# /opt/SUNWsgdg/bin/gateway config list
binding: *:443
routes-http-maxcon: 100
routes-aip-maxcon: 2920
routes-reverseproxy-redirect: null
services-reflection-binding: localhost:81
services-reflection-auth-binding: *:82
```

gateway config edit

SGD Gateway の現在の設定を編集します。

形式

```
gateway config edit [ --binding int:port ]
                    [ --routes-http-maxcon num ]
                    [ --routes-aip-maxcon num ]
                    [ --routes-reverseproxy-redirect port ]
                    [ --services-reflection-binding int:port ]
                    [ --services-reflection-auth-binding int:port ]
```

説明

コマンド行オプションを使用すると、特定の設定を編集できます。少なくとも 1 つのコマンド行オプションを指定する必要があります。

SGD Gateway の現在の設定は `/opt/SUNWsgdg/etc/gatewayconfig.xml` ファイルに保存されています。

設定に加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--binding`	SGD Gateway が着信プロキシ接続を待機するインタフェースとポート。デフォルトは、すべてのインタフェースの TCP ポート 443 です。
`--routes-http-maxcon`	HTTP 接続の最大数。デフォルト値は、SGD Gateway で使用可能なメモリー資源に応じてインストール時に設定されます。 63 ページの「 SGD Gateway の調整 」を参照してください。
`--routes-aip-maxcon`	AIP 接続の最大数。デフォルト値は、SGD Gateway で使用可能なメモリー資源に応じてインストール時に設定されます。 63 ページの「 SGD Gateway の調整 」を参照してください。
`--routes-reverseproxy-redirect`	HTTP リダイレクトポート。デフォルトの TCP ポートは 8080 です。
`--services-reflection-binding`	SGD Gateway リフレクションサービスに対する無認証アクセスに使用されるインタフェースとポート。デフォルトは、localhost ループバックインタフェースの TCP ポート 81 です。
`--services-reflection-auth-binding`	SGD Gateway リフレクションサービスに対する認証アクセスに使用されるインタフェースとポート。デフォルトは、すべてのインタフェースの TCP ポート 82 です。

使用例

次の例では、SGD Gateway の HTTP 接続と AIP 接続の最大数を変更します。

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-http-maxcon 200
# /opt/SUNWsgdg/bin/gateway config edit --routes-aip-maxcon 3000
```

gateway config enable

1 つ以上の SGD Gateway サービスを有効にします。

形式

```
gateway config enable [ --services-reflection ]
                      [ --services-reflection-auth ]
                      [ --routes-http-redirect ]
```

説明

特定の SGD Gateway サービスを有効にするには、コマンド行オプションを使用します。少なくとも 1 つのコマンド行オプションを指定する必要があります。

注 - このコマンドを使用してサービスを有効にしたあと、SGD Gateway を再起動してサービスを起動する必要があります。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--services-reflection`	SGD Gateway リフレクションサービスに対する無認証アクセスを有効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、71 ページの「リフレクションサービス」を参照してください。
`--services-reflection-auth`	SGD Gateway リフレクションサービスに対する認証アクセスを有効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、71 ページの「リフレクションサービス」を参照してください。
`--routes-http-redirect`	HTTP リダイレクトサービスを有効にします。 デフォルトでは、このサービスは無効になっています。

使用例

次の例では、SGD Gateway リフレクションサービスに対する認証アクセスを有効にします。

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection-auth
```

gateway config disable

1 つ以上の SGD Gateway サービスを無効にします。

形式

```
gateway config disable [ --services-reflection ]
                       [ --services-reflection-auth ]
                       [ --routes-http-redirect ]
```

説明

特定の SGD Gateway サービスを無効にするには、コマンド行オプションを使用します。少なくとも 1 つのコマンド行オプションを指定する必要があります。

注 - このコマンドを使用してサービスを無効にしたあと、SGD Gateway を再起動してサービスを停止する必要があります。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--services-reflection`	SGD Gateway リフレクションサービスに対する無認証アクセスを無効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、71 ページの「リフレクションサービス」を参照してください。
`--services-reflection-auth`	SGD Gateway リフレクションサービスに対する認証アクセスを無効にします。 デフォルトでは、このサービスは無効になっています。 SGD Gateway リフレクションサービスの詳細については、71 ページの「リフレクションサービス」を参照してください。
`--routes-http-redirect`	HTTP リダイレクトサービスを無効にします。 デフォルトでは、このサービスは無効になっています。

使用例

次の例では、SGD Gateway リフレクションサービスに対する認証アクセスを無効にします。

```
# /opt/SUNWsgdg/bin/gateway config disable --services-reflection-auth
```

gateway server

SGD サーバーに SGD Gateway の使用を承認します。

形式

```
gateway server add | remove | list
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
add	SGD サーバーに SGD Gateway の使用を承認します	42 ページの「 gateway server add 」
remove	SGD サーバーに対して SGD Gateway の使用の承認を削除します	44 ページの「 gateway server remove 」
list	SGD Gateway の使用を承認されている SGD サーバーを一覧表示します	45 ページの「 gateway server list 」

使用例

次の例では、SGD サーバー sgd.example.com に対して、SGD Gateway の使用の承認を削除します。

```
# /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
```

gateway server add

SGD サーバーに SGD Gateway の使用を承認します。

形式

```
gateway server add --server server-name
                   --certfile cert-file
                   --url server-url
                 [ --ssl-certfile ssl-cert ]
```

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--server`	SGD サーバーの DNS 名
`--cert-file`	SGD サーバーの認証局 (CA) 証明書
`--url`	SGD Web サーバーの URL (Uniform Resource Locator)
`--ssl-certfile`	SGD サーバーの SSL 証明書

`gateway server add` コマンドは次の処理を実行します。

- SGD サーバーの CA 証明書を SGD Gateway キーストア `/opt/SUNWsgdg/proxy/etc/keystore` にインポートします。CA 証明書は、`--server` オプションで指定された SGD サーバーと同じ名前の別名でキーストアに保存されます。
- SGD サーバーの SSL 証明書を SGD Gateway キーストア `/opt/SUNWsgdg/proxy/etc/keystore` にインポートします。SSL 証明書は、`--server` オプションで指定された SGD サーバーの名前に「 -ssl 」を付加した別名でキーストアに保存されます。
- Apache 逆プロキシサーバーで使用される負荷分散グループに SGD サーバーを追加します。

注 - `gateway server add` を使用したあと、変更を有効にするには SGD Gateway を再起動する必要があります。

使用例

次の例では、CA 証明書 PeerCAcert.pem を sgd.example.com という別名で SGD Gateway キーストアに追加します。SSL 証明書 cert.pem も sgd.example.com-ssl という別名でキーストアに追加されます。

```
# /opt/SUNWsgdg/bin/gateway server add --server sgd.example.com \
--certfile PeerCAcert.pem \
--url https://sgd.example.com \
--ssl-certfile cert.pem
```

この例では、SGD Web サーバーの URL https://sgd.example.com を逆プロキシの負荷分散グループに追加し、/opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/servers/conf/sgd.example.com.conf に設定ファイルを作成します。

gateway server remove

SGD サーバーに対して SGD Gateway の使用の承認を削除します。

形式

```
gateway server remove --server server-name
```

説明

SGD サーバーの CA 証明書と SSL 証明書を SGD Gateway キーストアから削除します。

注 - gateway server remove を使用したあと、変更を有効にするには SGD Gateway を再起動する必要があります。

使用例

次の例では、SGD サーバー sgd.example.com に対して、SGD Gateway の使用の承認を削除します。

```
# /opt/SUNWsgdg/bin/gateway server remove --server sgd.example.com
```

gateway server list

SGD Gateway の使用を承認されている SGD サーバーの詳細を表示します。

形式

```
gateway server list
```

説明

このコマンドは、SGD Gateway の使用を承認されている SGD サーバーの証明書の詳細と URL を表示します。

使用例

次の例では、SGD Gateway の使用を承認されている SGD サーバーの詳細を一覧表示します。

```
# /opt/SUNWsgdg/bin/gateway server list
```

gateway status

SGD Gateway の現在のステータスを表示します。

形式

```
gateway status
```

説明

このコマンドは、SGD Gateway が起動しているか停止しているか、あるいは問題が発生しているかを示します。

使用例

次の例では、SGD Gateway のステータス情報を表示します。この例で、SGD Gateway は停止しています。

```
# /opt/SUNWsgdg/bin/gateway status
SGD Gateway status: STOPPED
```

gateway version

SGD Gateway ソフトウェアのバージョン番号を表示します。

形式

```
gateway version
```

説明

SGD Gateway のバージョン番号を表示します。

使用例

次の例では、コマンドを実行するホストにインストールされている SGD Gateway のバージョンを表示します。

```
# /opt/SUNWsgdg/bin/gateway version
Oracle Secure Global Desktop Gateway 4.50.301
```

gateway sslcert

クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力またはエクスポートします。

形式

```
gateway sslcert export | print
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
export	クライアントキーストアから SGD Gateway の SSL 証明書をエクスポートします。	47 ページの「 gateway sslcert export 」
print	クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力します。	48 ページの「 gateway sslcert print 」

使用例

次の例では、クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力します。

```
# /opt/SUNWsgdg/bin/gateway sslcert print
```

gateway sslcert export

クライアントキーストアから SGD Gateway の SSL 証明書をエクスポートします。

形式

```
gateway sslcert export --certfile cert-file
```

説明

クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client から SGD Gateway の SSL 証明書をエクスポートします。証明書は、--certfile オプションで指定されたファイルに書き出されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用してクライアントキーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

使用例

次の例では、クライアントキーストアから SGD Gateway の SSL 証明書をファイル gateway-ssl.pem にエクスポートします。

```
# /opt/SUNWsgdg/bin/gateway sslcert export --certfile gateway-ssl.pem
```

gateway sslcert print

SGD Gateway の SSL 証明書を出力します。

形式

```
gateway sslcert print
```

説明

クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client に保存されている SGD Gateway の SSL 証明書を出力します。

このコマンドは、証明書の詳細を端末ウィンドウに書き出します。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用してクライアントキーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

使用例

次の例では、クライアントキーストアに保存されている SGD Gateway の SSL 証明書を出力します。

```
# /opt/SUNWsgdg/bin/gateway sslcert print
```

gateway sslkey

クライアントキーストア内の SSL キーおよび証明書のエントリを管理します。

形式

```
gateway sslkey import | export
```

説明

次の表は、このコマンドで使用可能なサブコマンドを示しています。

サブコマンド	説明	詳細情報
import	非公開鍵と証明書をクライアントキーストアにインポートします	49 ページの「 gateway sslkey import 」
export	クライアントキーストアから非公開鍵をエクスポートします	51 ページの「 gateway sslkey export 」

使用例

次の例では、クライアントキーストアに保存されている SGD Gateway の SSL 証明書をエクスポートします。

```
# /opt/SUNWsgdg/bin/gateway sslkey export --keyfile gateway-ssl.key
```

gateway sslkey import

SSL キーと証明書をクライアントキーストアにインポートします。

形式

```
gateway sslkey import --keyfile key-file
                      [ --keyalg RSA|DSA ]
                      { --certfile cert-file |
                        --certfile cert-file.. [ --cacertfile ca-cert-file ] }
                      [ --alwaysoverwrite ]
```

説明

SSL 非公開鍵とそれに対応する SSL 証明書を、クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client にインポートします。デフォルトでは、このキーストアには自己 署 名付き証明書が 1 つ入っています。

クライアントキーストアにすでにエントリが存在する場合、このコマンドによって上書きされます。デフォルトでは、キーストアのエントリを上書きする前に確認を求めるメッセージが表示されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用してクライアントキーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--keyfile	SSL 非公開鍵を含んでいるファイル。この鍵は Privacy Enhanced Mail (PEM) 形式で作成されている必要があります。
--keyalg	非公開鍵で使用する符号化アルゴリズム。オプションは RSA およびデジタル 署 名アルゴリズム (DSA) です。デフォルトでは、RSA が選択されます。
--certfile	SSL 証明書ファイル。
--cacertfile	CA 証明書またはルート証明書ファイル。
--alwaysoverwrite	確認を求めずにクライアント キースト アのエントリ を 上書きします。

証明書チェーンをインポートするには、--cacertfile オプションを使用して中間 CA の証明書を指定します。チェーン内の証明書はすべて PEM 形式で作成されている必要があります。

証明書チェーンで複数の CA 証明書が使用されている場合は、チェーン内のすべての CA 証明書を結合して 1 つのファイルにします。サーバー証明書の 署 名に使用される CA 証明書が最初に表示される必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
. . .Intermediate CA's certificate. . .
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
. . .CA root certificate. . .
-----END CERTIFICATE-----
```

使用例

次の例では、RSA で符号化された SSL 非公開鍵 gateway1-ssl.key とそれに対応する SSL 証明書 gateway1-ssl.pem をクライアント キースト アにインポート します。

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile gateway1-ssl.key \
--certfile gateway1-ssl.pem
```

次の例では、RSA で符号化された SSL 非公開鍵と SSL 証明書チェーンをクライアントキーストアにインポートします。中間 CA の証明書は gateway1-ca.pem です。

```
# /opt/SUNWsgdg/bin/gateway sslkey import \
--keyfile gateway1-ssl.key \
--certfile gateway1-ssl.pem \
--cafile gateway1-ca.pem
```

gateway sslkey export

クライアントキーストアから SGD Gateway の SSL 非公開鍵をエクスポートします。

形式

```
gateway sslkey export --keyfile key-file [ --keypass passwd ]
```

説明

クライアントキーストア /opt/SUNWsgdg/proxy/etc/keystore.client から SGD Gateway の SSL 非公開鍵をエクスポートします。非公開鍵は、--keyfile オプションで指定されたファイルに書き出されます。

--keypass オプションを使用して非公開鍵のパスワードを指定できます。デフォルトでは、/opt/SUNWsgdg/etc/password にあるパスワードが使用されます。

使用例

次の例では、クライアントキーストアから SGD Gateway の SSL 非公開鍵をファイル gateway-ssl.key にエクスポートします。

```
# /opt/SUNWsgdg/bin/gateway sslkey export --keyfile gateway-ssl.key
```

gateway cert export

SGD Gateway キーストアから SGD Gateway の証明書をエクスポートします。

形式

```
gateway cert export --certfile file-name
```

説明

SGD Gateway キーストア /opt/SUNWsgdg/proxy/etc/keystore から SGD Gateway の証明書をエクスポートします。証明書は、--certfile オプションで指定されたファイルに書き出されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用して SGD Gateway キーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

使用例

次の例では、SGD Gateway キーストアから SGD Gateway の証明書をファイル gateway1.pem にエクスポートします。

```
# /opt/SUNWsgdg/bin/gateway cert export --certfile gateway1.pem
```

gateway key import

SGD Gateway の鍵と SGD Gateway の証明書を SGD Gateway キーストアにインポートします。

形式

```
gateway key import --keyfile key-file
                   [ --keyalg RSA|DSA ]
                   { --certfile cert-file |
                     --certfile cert-file.. [ --cacertfile ca-cert-file ] }
                   [ --alwaysoverwrite ]
```

説明

非公開鍵とそれに対応する公開鍵証明書を、SGD Gateway キーストア /opt/SUNWsgdg/proxy/etc/keystore にインポートします。

キーストアにすでに SGD Gateway の鍵のエントリが存在する場合、そのエントリは上書きされます。デフォルトでは、確認を求めるメッセージが表示されます。

このコマンドは、/opt/SUNWsgdg/etc/password 内のパスワードを使用して SGD Gateway キーストアにアクセスします。このファイルが存在しない場合、パスワードの入力が求められます。

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--keyfile	非公開鍵を含んでいるファイル。鍵は PEM 形式で作成されている必要があります。
--keyalg	非公開鍵で使用する符号化アルゴリズム。オプションは RSA および DSA です。デフォルトでは、RSA が選択されます。
--certfile	SSL 証明書ファイル。
--cacertfile	CA またはルート証明書ファイル。
--alwaysoverwrite	確認を求めずにキーストアのエントリを上書きします。

証明書チェーンをインポートするには、--cacertfile オプションを使用して中間 CA の証明書を指定します。チェーン内の証明書はすべて PEM 形式で作成されている必要があります。

証明書チェーンで複数の CA 証明書が使用されている場合は、チェーン内のすべての CA 証明書を結合して 1 つのファイルにします。サーバー証明書の 署 名に使用される CA 証明書が最初に表示される必要があります。次に例を示します。

```
-----BEGIN CERTIFICATE-----
...Intermediate CA's certificate...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...CA root certificate...
-----END CERTIFICATE-----
```

使用例

次の例では、RSA で符号化された非公開鍵 `gateway1.key` と、それに対応する公開鍵証明書 `gateway1.pem` を、SGD Gateway キーストアにインポートします。

```
# /opt/SUNWsgdg/bin/gateway key import \
--keyfile gateway1.key \
--certfile gateway1.pem
```

次の例では、非公開鍵と証明書チェーンを SGD Gateway キーストアにインポートします。中間 CA の証明書は `gateway1-ca.pem` です。

```
# /opt/SUNWsgdg/bin/gateway key import \
--keyfile gateway1.key \
--certfile gateway1.pem \
--cafile gateway1-ca.pem
```

gateway setup

SGD Gateway のセットアッププログラムを実行します。

形式

```
gateway setup
```

説明

画面上の質問に回答して、SGD Gateway で使用するポート、インタフェース、およびセキュリティーを設定します。

使用例

次の例では、SGD Gateway のセットアッププログラムを実行します。

```
# /opt/SUNWsgdg/bin/gateway setup
```

gateway uninstall

SGD Gateway ソフトウェアをアンインストールします。

形式

```
gateway uninstall
```

説明

SGD Gateway を停止し、すべての設定情報も含めて SGD Gateway ソフトウェアを削除します。

SGD Gateway を停止する前に、このコマンドはユーザーに確認を求めます。

使用例

次の例では、コマンドを実行するホストから SGD Gateway ソフトウェアをアンインストールします。

```
# /opt/SUNWsgdg/bin/gateway uninstall
```

tarantella gateway コマンド

tarantella gateway コマンドは、SGD アレイの承認済みゲートウェイを設定するために使用します。

形式

```
tarantella gateway add | list | remove
```

説明

tarantella gateway コマンドを使用すると、SGD アレイのゲートウェイを追加、削除、および一覧表示できます。

tarantella gateway コマンドは、アレイ内の任意の SGD サーバー上で使用できます。加えた変更は、ほかのアレイメンバーに自動的に複製されます。

SGD サーバーがアレイに追加されると、プライマリ SGD サーバー上で定義されているゲートウェイセットがこの新しいアレイメンバーにコピーされます。承認済みゲートウェイがすでに存在している場合、それらはすべて上書きされます。SGD サーバーをアレイから切り離しても、登録済みゲートウェイが SGD サーバーから削除されることはありません。

使用可能な gateway コマンドのサブコマンドを次の表に示します。

サブコマンド	説明	詳細情報
add	SGD アレイの SGD Gateway を追加します	57 ページの「 tarantella gateway add 」
list	SGD アレイの SGD Gateway を一覧表示します	58 ページの「 tarantella gateway list 」
remove	SGD アレイの SGD Gateway を削除します	58 ページの「 tarantella gateway remove 」

注 - どの tarantella gateway サブコマンドにも --help オプションがあります。このオプションを使用すると、サブコマンドのヘルプを表示できます。

使用例

次の例では、SGD アレイの登録済みゲートウェイのリストに gateway1.example.com を追加します。

```
$ tarantella gateway add --name gateway1.example.com \
--certfile /opt/gateway1_cert_file.pem
```

tarantella gateway add

SGD Gateway を SGD アレイに登録します。

形式

```
tarantella gateway add {
                        --name server-name
                        --certfile cert-file
                        } | --file file
```

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
--name	登録する SGD Gateway の名前。
--certfile	SGD サーバーで使用する SGD Gateway の証明書。Definite Encoding Rules (DER) 形式または PEM 形式の証明書を使用できます。
--file	複数の SGD Gateway の設定を含んでいるバッチファイル。

使用例

次の例では、SGD アレイの登録済みゲートウェイのリストに gateway1.example.com を追加します。

```
$ tarantella gateway add --name gateway1.example.com \
--certfile /opt/gateway1_cert_file.pem
```

次の例では、tarantella gateway add の --file オプションを使用して、複数のゲートウェイを同時に登録します。

```
$ tarantella gateway add --file gateways.list
```

--file オプションでバッチファイル gateways.list を指定しています。このファイルには、次のように各ゲートウェイの設定の行が含まれています。

```
--name gateway1.example.com --certfile /opt/gateway1_cert_file.pem
--name gateway2.example.com --certfile /opt/gateway2_cert_file.pem
```

tarantella gateway list

SGD アレイに登録されている SGD Gateway を一覧表示します。

形式

```
tarantella gateway list
```

説明

`tarantella gateway add` コマンドを使用して SGD アレイに登録された SGD Gateway の詳細を表示します。

使用例

次の例では、SGD アレイの登録済みゲートウェイを一覧表示します。

```
$ tarantella gateway list
```

tarantella gateway remove

SGD アレイの登録済みゲートウェイのリストから、SGD Gateway を削除します。

形式

```
tarantella gateway remove --name server-name | --file file
```

説明

次の表は、このコマンドで使用可能なオプションを示しています。

オプション	説明
`--name`	登録の詳細を削除する SGD Gateway の名前
`--file`	複数の SGD Gateway の設定を含んでいるバッチファイル

使用例

次の例では、SGD アレイの登録済みゲートウェイのリストから、SGD Gateway `gateway1.example.com` を削除します。

```
$ tarantella gateway remove --name gateway1.example.com
```

--security-gateway 属性

`--security-gateway` 属性は、SGD アレイで SGD Gateway を使用できるようにするために使用します。この属性は、SGD Gateway にアクセスできる SGD Client を、クライアントの IP アドレスまたは DNS 名に基づいて定義します。

`--security-gateway` 属性に加えた変更は、アレイ内のすべての SGD サーバーに適用されます。

この属性の構文は次のとおりです。

```
--security-gateway filter-spec...
```

この *filter-spec* は、次の形式のフィルタ仕様で置き換えます。

```
client-ip-address | *:gateway protocol:gateway-address:gateway-port
```

ここで、*client-ip-address* は SGD Client の IP アドレスです。アスタリスク * はすべての IP アドレスを表します。SGD Gateway 経由の接続の場合、アレイ内の SGD サーバーはこのアドレスを使用して SGD Gateway に接続します。

注 - SGD Gateway とともに外部ロードバランサを使用している場合、*client-ip-address* にはロードバランサのアドレスを入力します。

---

gateway protocol は、SGD Gateway 経由の接続の場合は `sgdg` で、SGD Gateway を経由せずに SGD アレイに直接接続する SGD Client の場合は `direct` です。

gateway-address は、SGD Gateway または外部ロードバランサ (使用している場合) の外部アドレスです。クライアントデバイスはこのアドレスを使用して SGD Gateway に接続します。

gateway-port は、クライアントが SGD Gateway または外部ロードバランサ (使用している場合) に接続するために使用するポートです。

複数の *filter-spec* エントリは「 ; 」文字で区切ります。

次の例では、すべての SGD Client が SGD Gateway `gateway1.example.com` の TCP ポート 443 を使用して接続できるようにします。

```
$ tarantella config edit --security-gateway "*:sgdg:gateway1.example.com:443"
```

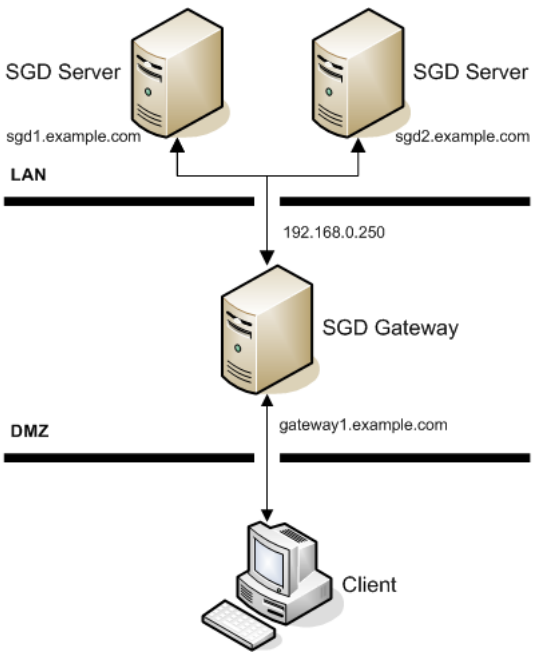
次の例では、すべての SGD Client が外部ロードバランサ `lb.example.com` を使用して接続できるようにします。

```
$ tarantella config edit --security-gateway \
"*:sgdg:lb.example.com:443"
```

次に例に示すように、複数のフィルタ仕様を使用できます。

図 B-1 に示す基本的な配備について考えましょう。この配備では、単一の SGD Gateway `gateway1.example.com` と、2 つの SGD サーバー `sgd1.example.com` および `sgd2.example.com` を含む SGD アレイが使用されます。内部ネットワーク上の SGD Gateway のアドレスは `192.168.0.250` です。

図 B-1 複数のフィルタ仕様の使用



この例には、次のようなフィルタ仕様を使用できます。

```
"192.168.0.250:sgdg:gateway1.example.com:443; \
*:direct:sgd1.example.com:80"
```

この設定により、次の内容が適用されます。

- アレイ内の SGD サーバーに対する接続は、SGD Gateway の IP アドレス `192.168.0.250` から許可されます。組織外部の SGD Client は、SGD Gateway `gateway1.example.com` の TCP ポート 443 を使用して接続します。
- ローカルエリアネットワーク (LAN) 上の SGD Client など、ほかの SGD Client はすべて SGD サーバー `sgd1.example.com` の TCP ポート 80 に直接接続します。これらの接続では SGD Gateway は使用されません。
- フィルタの順番は重要です。フィルタの順番を逆にすると、すべての SGD Client が SGD サーバー `sgd1.example.com` に直接接続するようになります。

付録 C

詳細設定

この章では、Oracle Secure Global Desktop Gateway (SGD Gateway) の高度な機能の設定と使用法について説明します。

この章の内容は、次のとおりです。

- 63 ページの「 SGD Gateway の調整 」
- 66 ページの「 HTTP リダイレクトの設定 」
- 66 ページの「 SGD Gateway のバインディングポートの変更 」
- 67 ページの「 SGD アレイに対する非暗号化接続の使用 」
- 68 ページの「外部 SSL アクセラレータの使用 」
- 69 ページの「 SGD Gateway でのクライアント証明書の使用法 」
- 70 ページの「 Balancer Manager アプリケーションの有効化 」
- 71 ページの「リフレクションサービス 」

SGD Gateway の調整

SGD Gateway のインストール時に、SGD Gateway ホストで使用可能なメモリーに応じて、Adaptive Internet Protocol (AIP) およびハイパーテキスト転送プロトコル (HTTP) の同時接続の最大数が自動的に設定されます。SGD Gateway の Java 仮想マシン (JVM™) に割り当てられるメモリーサイズも、この接続数に応じて最適化されます。

SGD Gateway のインストール後に、見込まれる SGD ユーザー数およびこれらのユーザーが実行するアプリケーションの数に応じて、デフォルトの設定を調整できます。その際は、JVM のメモリーサイズも調整する必要があります。この処理は、SGD Gateway の*「調整」*と呼ばれます。

注意 - 見込まれる接続数に対して JVM のメモリーサイズが不足すると、SGD Gateway が動作しなくなり、それ以降の接続をすべて拒否する場合があります。この場合は、十分な JVM メモリーが使用できるように SGD Gateway を調整する必要があります。
SGD Gateway で `java.lang.OutOfMemoryError` のエラーメッセージが表示された場合は、調整が必要な可能性があります。

SGD Gateway を調整するには、次の作業を実行します。

- AIP 接続の最大数を変更します。64 ページの「 AIP 接続の最大数の変更 」を参照してください。
- HTTP 接続の最大数を変更します。65 ページの「 HTTP 接続の最大数の変更 」を参照してください。
- JVM のメモリーサイズを変更します。65 ページの「 JVM のメモリーサイズの変更」を参照してください。

AIP 接続の最大数の変更

AIP 接続の最大数はインストール時に設定されます。デフォルトの設定は、SGD Gateway ホストで使用可能なメモリー資源によって異なります。

使用している配備に応じて、この設定をより適した値に変更できます。SGD Gateway で使用される AIP 接続の最大数を計算する方法の詳細については、64 ページの「 AIP 接続数の計算 」を参照してください。

AIP 接続の最大数を変更するには、`gateway config edit` コマンドの `--routes-aip-maxcon` オプションを使用します。たとえば、AIP 接続の最大数を 3000 に変更するには、次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-aip-maxcon 3000
```

加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

AIP 接続数の計算

SGD Gateway で使用される AIP 接続の数は、同時に接続する SGD ユーザーの数およびこれらのユーザーが実行するアプリケーションの数によって異なります。

AIP 接続数 = (*アプリケーション数* + 3) x *SGD ユーザー数*

たとえば、SGD Gateway で 1000 人の SGD ユーザーがそれぞれ 4 つのアプリケーションを実行する場合、必要な AIP 同時接続の最大数は次のようになります。

(4 + 3) x 1000 = 7000 AIP 接続

HTTP 接続の最大数の変更

HTTP 接続の最大数はインストール時に設定されます。デフォルト値は 100 です。

HTTP 接続の最大数を変更するには、`gateway config edit` コマンドの `--routes-http-maxcon` オプションを使用します。たとえば、HTTP 接続の最大数を 200 に変更するには、次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway config edit --routes-http-maxcon 200
```

加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

JVM のメモリーサイズの変更

HTTP 接続と AIP 接続の最大数を変更する場合は、SGD Gateway の JVM に割り当てられているメモリーサイズの変更も必要になることがあります。そのためには、`/opt/SUNWsgdg/proxy/etc/tuning_parameters` ファイルで次の設定を編集します。

- `-Xms` – JVM の初期メモリーサイズ
- `-Xmx` – JVM の最大メモリーサイズ

これらの値を計算する方法の詳細については、65 ページの「 JVM のメモリーサイズの計算 」を参照してください。

注 - JVM の設定に対して十分なメモリー資源がシステムに設定されていることを確認してください。

加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

JVM のメモリーサイズの計算

SGD Gateway で使用される JVM メモリーの量は、AIP および HTTP の同時接続数によって異なります。

各 SGD Gateway 接続に約 300K バイトの JVM メモリーが必要なので、必要な JVM メモリーは次のように求められます。

(*AIP 接続数* + *HTTP 接続数*) x 300K バイト

たとえば、SGD Gateway で 500 人の SGD ユーザーがそれぞれ 2 つのアプリケーションを実行するとします。 AIP 同時接続の最大数は次のようになります。

(2 + 3) x 500 = 2500 AIP 接続

SGD Gateway では、SGD Web サーバーに対する十分な数の HTTP 同時接続も処理する必要があります。この例では、HTTP 接続の最大数は次のとおりです。

250 HTTP 接続

したがって、必要な JVM メモリーは次のようになります。

(2500 + 250) x 300K バイト = 約 806M バイト

注 - `/opt/SUNWsgdg/proxy/etc/tuning_parameters` ファイルで、`-Xms` と `-Xmx` を、計算された JVM メモリー値に設定します。パフォーマンスの理由から、`-Xms` と `-Xmx` は通常は同じ値に設定されます。

HTTP リダイレクトの設定

デフォルトでは、SGD Gateway は Transmission Control Protocol (TCP) ポート 80 での HTTP 接続を拒否します。

TCP ポート 80 での接続を有効にするには、次のように `gateway config enable` コマンドを使用して HTTP リダイレクトサービスを有効にします。

```
# /opt/SUNWsgdg/bin/gateway config enable --routes-http-redirect
```

加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

SGD Gateway のバインディングポートの変更

SGD Gateway で着信接続に使用されるインタフェースとポートは、*「バインディングポート」*と呼ばれます。デフォルトでは、SGD Gateway はすべてのインタフェースで TCP ポート 443 をバインディングポートとして使用します。

バインディングポートを変更するには、`gateway config edit` コマンドの `--binding` オプションを使用します。たとえば、バインディングポートを TCP ポート 4443 に変更するには、次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway config edit --binding *:4443
```

または、SGD Gateway ホストで /opt/SUNWsgdg/bin/gateway config create コマンドを実行することによっても、バインディングポートを変更できます。このコマンドでは、着信プロキシ接続に使用するインタフェースとポートの入力が求められます。

注 - gateway config create コマンドを使用すると新しい設定が作成され、それまでに行なった設定はすべて上書きされます。

加えた変更を有効にするには、SGD Gateway を再起動する必要があります。

SGD アレイに対する非暗号化接続の使用

デフォルトでは、SGD Gateway とアレイ内の SGD サーバーの間の接続は、Secure Sockets Layer (SSL) を使用してセキュリティー保護されます。つまり、AIP over SSL データでは TCP ポート 5307 が使用され、HTTPS データでは TCP ポート 443 が使用されます。

SGD Gateway とアレイ内の SGD サーバーの間で非暗号化接続を使用するには、次のコマンドを実行します。

```
# gateway config create
```

SGD サーバーに対してセキュア接続を使用するかどうか質問されたら、n と入力します。

注 - アレイ内の SGD サーバーが標準の非暗号化接続を使用するように設定されていることを確認してください。そのためには、アレイ内の各 SGD サーバーで tarantella security stop コマンドを実行して、SGD セキュリティーサービスをオフにします。

非暗号化接続の場合、AIP データでは TCP ポート 3144 が使用され、HTTP データでは TCP ポート 80 が使用されます。

外部 SSL アクセラレータの使用

デフォルトでは、SGD Gateway は SSL でセキュリティー保護された HTTP および AIP の着信データ接続で動作するように設定されています。Gateway では、SSL の処理を行うために外部 SSL アクセラレータの使用もサポートされています。

Gateway で外部 SSL アクセラレータを使用するには、次の手順を実行します。

- SSL 接続を復号化し、それらを暗号化されていない接続として Gateway に転送するように外部 SSL アクセラレータを設定します。
- Gateway で外部 SSL アクセラレータのサポートを有効にします。

  これにより、セキュリティー保護されたポートで Gateway が暗号化されていない接続を受け入れることができるようになります。68 ページの「 外部 SSL アクセラレータのサポートを有効にする方法を参照してください。
- クライアントデバイスで SSL アクセラレータがネットワークのエントリポイントとして使用されていることを確認します。

  通常、SSL アクセラレータはロードバランサでもあります。9 ページの「負荷分散された配備」で説明されている負荷分散された配備に対して SGD サーバーと Gateway を設定します。

▼ 外部 SSL アクセラレータのサポートを有効にする方法

Gateway を経由して SGD に接続されているユーザーがいないことを確認します。

1. **SGD Gateway ホストにスーパーユーザー (root) としてログインします。**
2. **暗号化されていない着信接続のサポートを有効にします。**

   `gateway.xml` ファイルのシンボリックリンクを変更して、デフォルトの `gateway-ssl.xml` ではなく、`gateway-plaintext.xml` ファイルにリンクするようにします。

   次のコマンドを実行します。

```
# ln -fs /opt/SUNWsgdg/etc/gateway-plaintext.xml /opt/SUNWsgdg/etc/gateway.xml
```

3. **(省略可能) Gateway のバインディングポートを変更します。**

   ネットワークの設定によっては、SGD Gateway のバインディングポートを変更する必要がある場合もあります。

   66 ページの「 SGD Gateway のバインディングポートの変更」を参照してください。

4. **SGD Gateway を再起動します。**

```
# /opt/SUNWsgdg/bin/gateway restart
```

SGD Gateway でのクライアント証明書の使用法

*クライアント証明書*を使用して、有効な証明書を持っているユーザーにアクセスを制限することによって、SGD Gateway のセキュリティを向上させることができます。

クライアント証明書とは、クライアントデバイスのブラウザにインストールされる SSL 証明書です。クライアント証明書のインストール方法については、ブラウザのオンラインドキュメントを参照してください。

▼ クライアント証明書が使用されるように SGD Gateway を設定する方法

この手順を実行するには、クライアント証明書が必要です。

1. **SGD Gateway ホストにスーパーユーザー (root) としてログインします。**

2. **SGD Gateway を停止します。**

```
# /opt/SUNWsgdg/bin/gateway stop
```

3. **HTTPS クライアント接続にクライアント証明書が使用されるように、SGD Gateway を設定します。**

   次のように、<needClientAuth> エントリを /opt/SUNWsgdg/etc/gateway.xml ファイルに追加します。

```
<service id="http-ssl-service" class="SSL">
    <needClientAuth>true</needClientAuth>
        <!-- Decrypts HTTPS traffic -->
        <subService id="ssl-splitter">
            <binding>*</binding>
        </subService>
```

4. **クライアント証明書を SGD Gateway クライアントキーストアにインポートします。**

   keytool コマンドを次のように使用します。

```
# /opt/SUNWsgdg/java/default/bin/keytool -importcert \
-alias mycert -keystore /opt/SUNWsgdg/proxy/etc/keystore.client \
 -file mycert.crt -storepass 'cat /opt/SUNWsgdg/etc/password'
```

   この例では、クライアント証明書 mycert.crt が SGD Gateway クライアントキーストアにインポートされます。クライアント証明書は、mycert の別名で保存されます。

5. **SGD Gateway を起動します。**

```
# /opt/SUNWsgdg/bin/gateway start
```

Balancer Manager アプリケーションの有効化

Apache 逆プロキシには Balancer Manager という Web アプリケーションが含まれています。Balancer Manager では、逆プロキシで使用される負荷分散グループの SGD Web サーバーを管理できます。

Balancer Manager を使用すると、次の作業を実行できます。

- 負荷分散グループの SGD Web サーバーのステータス情報を表示する
- SGD Web サーバーの負荷分散の経路を表示および変更する
- 負荷分散グループから SGD Web サーバーを削除する

Balancer Manager を有効にするには、逆プロキシ設定ファイル /opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/httpd-gateway.conf でこのアプリケーションを無効にしているコメントを削除します。

```
# Allows the configuration of load balancing parameters
#
#    <Location /balancer-manager>
#        SetHandler balancer-manager
#        Order Deny,Allow
#        Deny from all
#        Allow from all
#    </Location>
```

加えた変更を有効にするには、逆プロキシを再起動する必要があります。

Balancer Manager にアクセスするには、ブラウザを起動して `https://` *gateway.example.com*`/balancer-manager` にアクセスします。ここで、*gateway.example.com* は SGD Gateway ホストです。

Balancer Manager については、**Apache mod_proxy_balancer のドキュメント** を参照してください。

リフレクションサービス

*「リフレクションサービス」*とは、SGD Gateway のルーティングプロキシコンポーネントで使用される RESTful Web サービスの集まりです。SGD Gateway 管理者はリフレクションサービスを使用して、ルーティングプロキシの経路、サービス、ログレベル、および接続を設定したり、ステータス情報を表示したりできます。

この節では、次に示すリフレクションサービス関連のトピックについて説明します。

- 71 ページの「リフレクションサービスの有効化」
- 74 ページの「リフレクションサービスの使用」

リフレクションサービスの有効化

デフォルトでは、SGD Gateway のリフレクションサービスは無効になっています。

次のアクセス方法の 1 つ以上に対してリフレクションサービスを有効にします。

- **無認証アクセス –** ユーザーは認証を受ける必要がありません。

  デフォルトでは、無認証アクセスを使用できるのは SGD Gateway ホストからだけです。

  無認証アクセスを有効にする方法の詳細については、72 ページの「リフレクションサービスに対する無認証アクセスを有効にする方法」を参照してください。

- **認証アクセス –** ユーザーはリフレクションサービスにアクセスする前に認証を受ける必要があります。

  認証アクセスを有効にする方法の詳細については、73 ページの「リフレクションサービスに対する認証アクセスを有効にする方法」を参照してください。

▼ リフレクションサービスに対する無認証アクセスを有効にする方法

1. SGD Gateway ホストにスーパーユーザー (root) としてログインします。

2. リフレクションサービスに対する無認証アクセスを有効にします。

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection
```

3. (省略可能) リフレクションサービスで使用するインタフェースを変更します。

注意 - デフォルトでは、リフレクションサービスに対する無認証アクセスを使用できるのは SGD Gateway ホストからだけです。ほかのインタフェースで無認証アクセスを有効にすると、セキュリティーリスクが発生する可能性があります。

リフレクションサービスに対する無認証アクセスに使用されるデフォルトのインタフェースは、`localhost` ループバックインタフェースです。次の例は、すべてのインタフェースで無認証アクセスを有効にする方法を示しています。

```
# /opt/SUNWsgdg/gateway config edit \
--services-reflection-binding *:81
```

4. (省略可能) リフレクションサービスで使用するポートを変更します。

リフレクションサービスに対する無認証アクセスに使用されるデフォルトのポートは、TCP ポート 81 です。これを別の未使用のポートに次の手順で変更できます。

```
# /opt/SUNWsgdg/gateway config edit \
--services-reflection-binding localhost:portnum
```

ここで、*portnum* はリフレクションサービスで使用するポート番号です。

5. SGD Gateway を再起動します。

```
# /opt/SUNWsgdg/bin/gateway restart
```

6. リフレクションサービスにアクセスします。

SGD Gateway ホストで、ブラウザを起動して `http://localhost:81` にアクセスします。

リフレクションサービスのホームページが表示されます。

▼ リフレクションサービスに対する認証アクセスを有効にする方法

1. **SGD Gateway ホストにスーパーユーザー (root) としてログインします。**

2. **リフレクションサービスの証明書と非公開鍵をエクスポートします。**

   リフレクションサービスの証明書と非公開鍵は、リフレクションサービスキーストア /opt/SUNWsgdg/proxy/etc/keystore.reflection に保存されています。このキーストアは、SGD Gateway のインストール時に自動的に作成されます。

   デフォルトでは、リフレクションサービスキーストアには自己 署 名付き証明書と鍵のペアが 1 つ入っています。

   a. **リフレクションサービスの証明書をエクスポートします。**

```
# /opt/SUNWsgdg/java/default/bin/keytool -exportcert \
-alias server-name -rfc \
-keystore /opt/SUNWsgdg/proxy/etc/keystore.reflection \
-storepass "$(cat /opt/SUNWsgdg/etc/password)" \
-file client.pem
```

   ここで、*server-name* はリフレクションサービスキーストアでリフレクションサービスの証明書に使用されている別名 、*client.pem* はエクスポートした証明書のファイル名です。

   b. **リフレクションサービスの非公開鍵をエクスポートします。**

   SGD Gateway に含まれている KeyManager アプリケーションを使用します。

```
# /opt/SUNWsgdg/java/default/bin/java \
-jar /opt/SUNWsgdg/proxy/KeyManager.jar export \
--keyfile client.key \
--keystore /opt/SUNWsgdg/proxy/etc/keystore.reflection \
--keyalias alias-name \
--keypass "$(cat /opt/SUNWsgdg/etc/password)" \
--storepass "$(cat /opt/SUNWsgdg/etc/password)"
```

   ここで、*alias-name* はリフレクションサービスキーストアでリフレクションサービスの鍵に使用されている別名 、*client.key* はエクスポートした鍵のファイル名です。

3. **証明書と非公開鍵をクライアントデバイスにインストールします。**

   証明書と非公開鍵は、リフレクションサービスに対する承認を得るためにクライアントデバイスで使用されます。

4. **リフレクションサービスに対する認証アクセスを有効にします。**

   SGD Gateway ホストで、次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway config enable --services-reflection-auth
```

5. **(省略可能) リフレクションサービスで使用するインタフェースとポートを変更します。**

   リフレクションサービスに対する認証アクセスに使用されるデフォルトのバインディングは、すべてのインタフェースの TCP ポート 82 です。これを別のインタフェースの未使用のポートに次の手順で変更できます。

```
# /opt/SUNWsgdg/gateway config edit \
--services-reflection-binding int:portnum
```

   ここで、*int* はインタフェース、*portnum* はリフレクションサービスで使用するポート番号です。

6. **SGD Gateway を再起動します。**

```
# /opt/SUNWsgdg/bin/gateway restart
```

7. **証明書と非公開鍵を使用して、クライアントデバイスからリフレクションサービスに接続します。**

```
$ curl --cert client.pem --key client.key -k -X GET https://gateway.example.com:82
```

   この例では、`curl` コマンドを使用してリフレクションサービスのホームページ `https://`*gateway.example.com*`:82` にアクセスします。ここで、*gateway.example.com* は SGD Gateway の名前です。リフレクションサービスの証明書と非公開鍵は、*client.pem* と *client.key* です。

リフレクションサービスの使用

リフレクションサービスによって提供されている RESTful Web サービスにアクセスするには、クライアントアプリケーションを使用します。適切なクライアントアプリケーションには次のようなものがあります。

- **ブラウザ:** リフレクションサービスにアクセスするもっとも簡単な方法は、ブラウザを使用することです。ただし、ブラウザでサポートされるのは HTTP `GET` 要求だけなので、情報を取り出す RESTful Web サービスにしかアクセスできません。実際、ブラウザを使用すると、ルーティングプロキシのステータス情報を表示したり、経路とサービスを一覧表示したりする作業に役立ちます。

- **curl:** これは UNIX および Linux プラットフォーム用のコマンド行ツールで、HTTP `GET` 、 `PUT` 、 `POST` 、および `DELETE` 要求をサポートしています。したがって、リフレクションサービスの全種類の RESTful Web サービスを使用できます。このツールの出力をファイルや別のプログラムにリダイレクトして、さらに処理することもできます。

または、RESTful Web サービスをサポートするユーザー独自のクライアントアプリケーションを持っている場合は、それを使用してリフレクションサービスにアクセスできます。

注 - リフレクションサービスを使用してルーティングプロキシの設定を変更する場合、SGD Gateway を再起動する必要はありません。

リフレクションサービスからは次の出力形式でデータが返されることがあります。

- **ASCII:** これはデフォルトの出力形式です。データはタブで区切られた ASCII 形式で返されます。この出力形式は、あとでデータに構文解析などの処理を行う場合に役立ちます。
- **HTML.:**データは、ブラウザでの表示に適したハイパーテキストマークアップ言語 (HTML) 形式で返されます。HTML 出力を取得するには、Web サービスの URI (Uniform Resource Identifier) の末尾に `/html` を付加します。

RESTful Web サービスについて

次の表に、SGD Gateway リフレクションサービスの RESTful Web サービスの一覧を示します。

相対 URI	HTTP 要求メソッド	説明
/	GET	ルーティングプロキシに関する稼働時間などの概要情報を表示します。
/service	GET	使用可能なサービスを一覧表示します。 サービスは、ルーティングプロキシが着信接続を行うエントリポイントです。
/service/*Service-Id*	GET	*Service-Id* で指定されたサービスの情報を一覧表示します。
/service/*Service-Id*	PUT	*Service-Id* で指定されたサービスを起動します。
/service/*Service-Id*	DELETE	*Service-Id* で指定されたサービスを停止します。
/client	GET	使用可能なクライアントを一覧表示します。 クライアントは、ルーティングプロキシが発信接続を行う出口ポイントです。

相対 URI	HTTP 要求メソッド	説明
/client/*Client-Id*	GET	*Client-Id* で指定されたクライアントの情報を一覧表示します。
/route	GET	使用可能な経路を一覧表示します。 経路は、サービス経由の着信接続から、クライアント経由の発信接続までの、ルーティングプロキシを通る経路です。
/route/*Route-Id*	GET	*Route-Id* で指定された経路の情報を一覧表示します。
/route/*Route-Id*	PUT	*Route-Id* で指定された経路を起動します。
/route/*Route-Id*	DELETE	*Route-Id* で指定された経路を停止します。
/route/*Route-Id*/connection	GET	*Route-Id* で指定された特定の経路の接続を一覧表示します。
/route/*Route-Id*/connection/*Connection-Id*	DELETE	*Connection-Id* で指定された接続を終了します。
/connection	GET	すべての経路について、現在実行中の接続を一覧表示します。
/logging/level	GET	グローバルなログレベルを表示します。
/logging/level/*Log-Level*	PUT	ルーティングプロキシのグローバルなログレベルを設定します。
/logging/*Package*/level	GET	ルーティングプロキシの特定のコンポーネントのログレベルを表示します。
/logging/*Package*/level/*Log-Level*	PUT	ルーティングプロキシの特定のコンポーネントのログレベルを設定します。

RESTful Web サービスにアクセスするには、リフレクションサービスの URL (Uniform Resource Locator) に Web サービスの相対 URI を付加します。

たとえば、SGD Gateway *gateway.example.com* の使用可能な経路を一覧表示するには、次のようにリフレクションサービスの URL に /route を付加します。

```
$ curl --cert client.pem --key client.key -k -X GET https://gateway.example.com:82/route
```

ここで、*client.pem* と *client.key* は、リフレクションサービスの証明書と非公開鍵です。この例では、クライアントはリフレクションサービスにアクセスする前に認証を受けます。

リフレクションサービスの使用例

次の例ではいずれも、リフレクションサービスにアクセスするためのクライアントアプリケーションとして curl を使用します。

これらの例では、*gateway.example.com* という SGD Gateway のリフレクションサービスに対して認証アクセスを使用します。クライアントは、証明書 *client.pem* および非公開鍵 *client.key* を使用して認証されます。

SGD Gateway の使用可能なサービスを一覧表示するには、次のコマンドを使用します。

```
$ curl --cert client.pem --key client.key -k \
-X GET https://gateway.example.com:82/service
```

経路を停止するには、リフレクションサービスでその経路に使用されている Route Id を指定します。

```
$ curl --cert client.pem --key client.key -k \
-X GET https://gateway.example.com:82/route
Route Id  Route Uptime   Service Id  ...
0         21h18m20s743m  ssgd-route-service  ...
1         21h18m20s736m  shttp-ssl-service   ...
$ curl --cert client.pem --key client.key -k \
-X DELETE https://gateway.example.com:82/route/1
```

グローバルなログレベルを FINER に設定するには、次のコマンドを使用します。

```
$ curl --cert client.pem --key client.key -k \
-X PUT https://gateway.example.com:82/logging/level/FINER
```

付録 D

SGD Gateway のトラブルシューティング

この章は、Oracle Secure Global Desktop Gateway (SGD Gateway) の問題の診断と解決に役立つ、トラブルシューティング関連のトピックから構成されます。

この章の内容は、次のとおりです。

- 79 ページの「 ログと診断 」
- 82 ページの「 SGD Gateway のエラーメッセージ 」

ログと診断

この節では、SGD Gateway のログ機能と診断機能について説明します。

ここで説明する内容は、次のとおりです。

- 79 ページの「 SGD Gateway のログについて 」
- 81 ページの「 SGD Gateway のプロセス情報の表示 」
- 81 ページの「 コマンド行からの設定の確認 」
- 82 ページの「 SGD Gateway のエラーメッセージ 」

SGD Gateway のログについて

SGD Gateway のログでは、Java Logging アプリケーションプログラミングインタフェース (API) が使用されます。Java での Java Logging の実装については、`http://java.sun.com/javase/6/docs/technotes/guides/logging/overview.html` を参照してください。

ログレベルの変更

SGD Gateway ではログプロパティー設定ファイル `logging.properties` が提供されています。このファイルは `/opt/SUNWsgdg/proxy/etc` ディレクトリにあります。

`logging.properties` ファイルを編集して、デフォルト のログレベルを変更したり、特定の SGD Gateway サービスのログレベルを設定したりできます。`logging.properties` ファイルでは、各 SGD Gateway サービスは `async.channel` エントリで表されます。

たとえば、Transmission Control Protocol (TCP) の着信接続と発信接続のログレベルを上げるには、TCP サービスのログレベルを `FINEST` に設定します。`logging.properties` ファイルで、次の行のコメントを解除します。

```
# async.channel.tcp.level=FINEST
```

`logging.properties` ファイルを編集してログレベルを変更した場合、変更を有効にするには SGD Gateway を再起動する必要があります。

注 - SGD Gateway リフレクションサービスを使用してログレベルを変更することもできます。リフレクションサービスの設定と使用については、71 ページの「リフレクションサービス」を参照してください。

ログファイルの場所

SGD Gateway に問題が発生した場合は、次のログファイルを調べてください。

- **ルーティングプロキシのログファイル。**これらのログファイルの場所と名前は、`logging.properties` ファイルで設定されます。デフォルトでは、SGD Gateway はルーティングプロキシのログファイルを SGD Gateway ホストの `/opt/SUNWsgdg/proxy/var/log` ディレクトリに作成します。
- **逆プロキシのログファイル。**HTTP 接続および HTTPS 接続の負荷分散およびプロキシサーバーのアクティビティーの詳細は、SGD Gateway ホストの `/opt/SUNWsgdg/httpd/apache-version/logs` ディレクトリの Apache ログファイルに記録されます。
- **SGD サーバーのログファイル。**アレイ内の各 SGD サーバーは、SGD サーバーホストの `/opt/tarantella/var/log` ディレクトリのログファイルにエラーメッセージを書き込みます。SGD サーバーのログ設定については、『*Oracle Secure Global Desktop 4.6 管理者ガイド*』の第 6 章の「監視とログ」を参照してください。

SGD Gateway のプロセス情報の表示

SGD Gateway の起動時に、ルーティングプロキシのプロセス ID が SGD Gateway ホスト上の `/opt/SUNWsgdg/proxy/var/run/proxy.pid` ファイルに保存されます。

逆プロキシのプロセス ID は `/opt/SUNWsgdg/httpd/apache-version/logs/httpd.pid` ファイルに保存されます。このファイルの場所は、`httpd.conf` Apache 設定ファイルの `PidFile` 指令を使用して変更できます。

実行中の SGD Gateway プロセスを表示するには、SGD Gateway ホストで次のコマンドを使用します。

```
# ps -ef | grep SUNWsgdg
```

コマンド行からの設定の確認

次のコマンドを使用して、SGD Gateway の設定を確認できます。

- `gateway status` – SGD Gateway のステータス情報を表示します。

  SGD Gateway ホストで次のコマンドを実行します。

```
# /opt/SUNWsgdg/bin/gateway status
```

  このコマンドの詳細については、45 ページの「 `gateway status` 」も参照してください。

- `tarantella gateway list` – SGD アレイで使用することを承認されている SGD Gateway のリストを表示します。

  アレイ内の任意の SGD サーバーで次のコマンドを実行します。

```
$ tarantella gateway list
```

  `tarantella gateway` コマンドの使用方法の詳細については、55 ページの「 `tarantella gateway` コマンド 」を参照してください。

- `tarantella config list` – SGD アレイのグローバル設定を表示します。

  任意の SGD サーバーで次のコマンドを実行して、`--security-gateway` 属性の設定を表示します。この属性により、SGD Gateway の使用を許可される SGD Client が決まります。

```
$ tarantella config list --security-gateway
```

  この属性の詳細については、59 ページの「 `--security-gateway` 属性 」を参照してください。

SGD Gateway のエラーメッセージ

SGD Gateway のエラーメッセージは、SGD Gateway ホストの `/opt/SUNWsgdg/proxy/var/log` ディレクトリにあるルーティングプロキシのログファイルに報告されます。

SGD Gateway の代表的なエラーメッセージのいくつかを、その推定原因の説明とともに次の表に示します。

エラーメッセージ	推定原因

`Failed to validate token:`
トークンの検証に失敗しました:
`Token time not yet valid`
トークンはまだ有効になっていません
	SGD Gateway とアレイ内の SGD サーバーのクロックが同期していません

`Failed to decode token:`
トークンの復号化に失敗しました:
`No trusted signature found`
信頼できる 署 名が見つかりません
	SGD サーバーの CA 証明書が SGD Gateway にインストールされていません

`Failed to validate token:`
トークンの検証に失敗しました:
`No recipient available to decrypt token`
トークンを復号化できる受信者がありません
	SGD Gateway の証明書が SGD アレイにインストールされていません

`SSL error:`
SSL エラー:
`Check the proxy SSL keystore has valid trusted certificates`
プロキシの SSL キーストアに有効な信頼できる証明書があることを確認してください
	SGD サーバーの SSL 証明書が SGD Gateway にインストールされていません